CHIP

CHIP tar

CHIP SPECIAL

16.

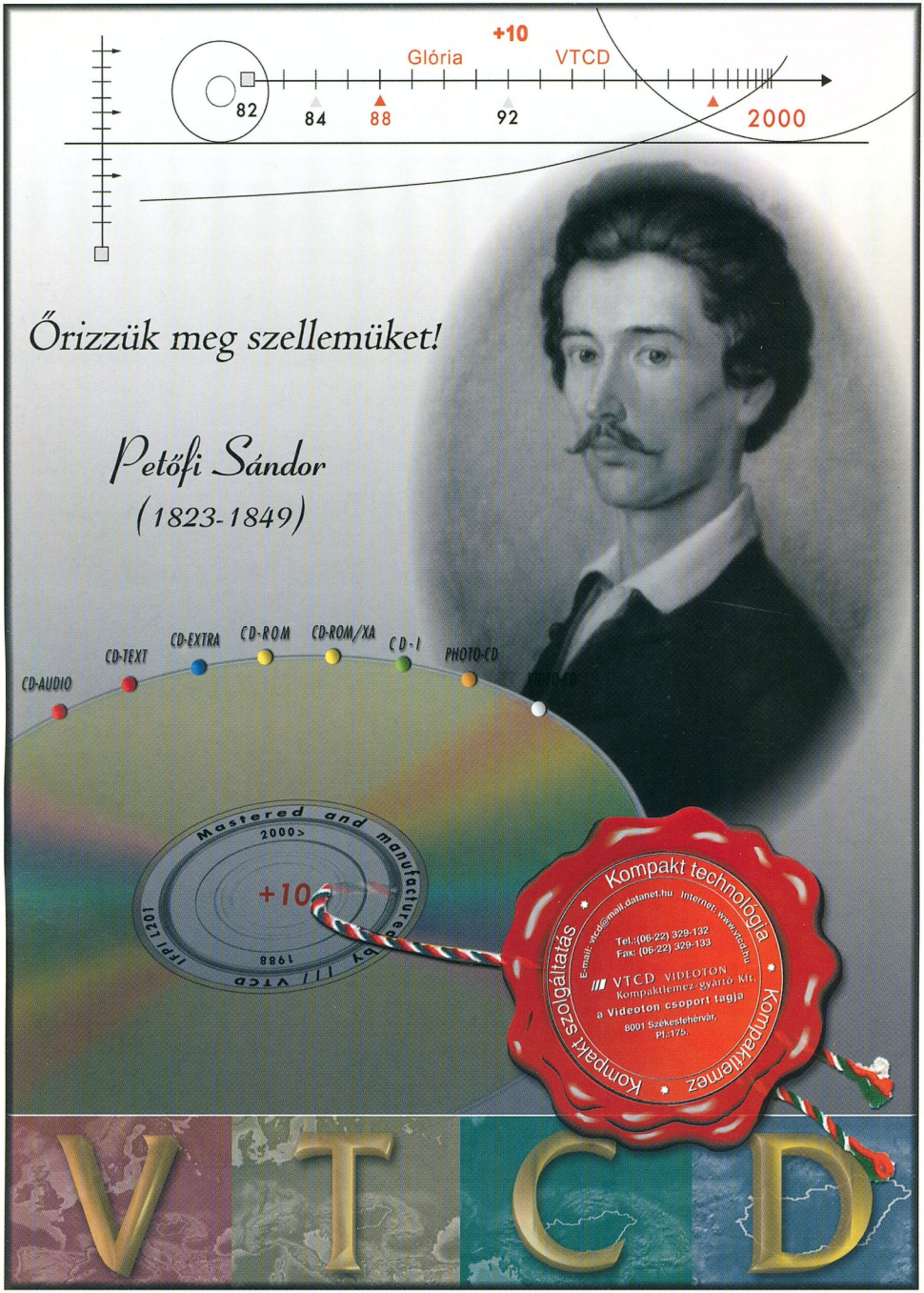
Ára: 1960 Ft

WINDOWS 2000

A CD-mellékleten: Windows 2000 Útikalauz

Újdonságok
Megbízhatóság
Biztonsági szolgáltatások
A szoftvertelepítő szolgáltatás
Csoportos házirend
Áttérés NT 4-ről
Smart Cardok

9 771219 432003 00016


+10
Glória
VTCD
82
84
88
92
2000
Őrizzük meg szellemüket!
Petőfi Sándor
(1823-1849)
CD-AUDIO
CD-TEXT
CD-EXTRA
CD-ROM
CD-ROM/XA
CD-I
PHOTO-CD
Mastered and manufactured by VTCD
2000>
+10
1988
Kompakt technológia
Kompaktlemez
Kompakt szolgáltatás
E-mail: vtcd@mail.datanet.hu Internet: www.vtcd.hu
Tel.:(06-22) 329-132
Fax: (06-22) 329-133
VTCD VIDEOTON
Kompaktlemez-gyártó Kft.
a Videoton csoport tagja
8001 Székesfehérvár,
Pf.:175.
V
T
C
D

Negyed százada tart a személyi számítógépek (Personal Computer – PC) diadalmenete. A hetvenes évek második felében olyasvalami történt, amit a sci-fikben sem jósoltak meg azelőtt: mindenkinek – persze legelőször a gazdagabbaknak – lehetett saját gépe, ami akár egy asztalon is elfért.

Az IBM PC térhódításával a korábbi ezerfajta, egymással szót nem értő PC-kezdemény kiveszett, s ebben az új, emberbarát operációs rendszer, a Windows is sokat segített.

A személyi gép új produktivitást adott az emberiségnek, a korábbi drága tudományos játékszerekből kéziszerszám lett a megfelelő kezekben. Mint azóta látjuk, a „kezek" száma folyamatosan nő. Mindemellett a masinák személyi volta egy idő után kezdett komoly akadállyá válni, a sok kis, egymással nem kommunikáló gép vállalati környezetben gyakran nem ért többet, mint egy-egy drága, rossz kihasználtságú, elektronikus kombináltfogó.

A központosított helyi hálózatok eleinte megoldást jelentettek a problémára, a gépén mindenki azt tehetett amit akart, a szerveren tartott adatok és alkalmazások a cég, illetve a rendszergazda hatáskörén belül maradtak. A 20–40 megabyte-os háttértárak kimúltakor és az Internet bejövetelével a szinte felderíthetetlen személyi szemétdombként is üzemelő PC-k egyre nagyobb gondot jelentettek a rendszergazdák számára. A csoportmunka-alkalmazásokkal kiteljesedő vállalati számítástechnika világában egyre több „szemet szúrt" a maga kis szemétdombján kakaskodó, megregulázhatatlan felhasználó. A szigorúbbnál szigorúbb számítástechnikai házirendeket jóformán csak az tartotta be, aki egymaga nem volt képes egy új alkalmazást telepíteni. Elkerülhetetlenné vált egy olyan operációs rendszer kifejlesztése, amely ugyan személyi marad, de a vállat igényeit is messzemenően figyelembe veszi.

A Microsoft a Windows NT-vel tette meg az első lépést a kívánt irányba. Az NT természetesen nem csak kliens oldali rendszerként jelent meg, a konzisztens vállalati rendszer megkövetelte a kiszolgáló változatot is. Az NT kiváló tulajdonságai mellett mégis sok mindent megörökölt a korábbi kliensrendszerek bajaiból: nem eléggé skálázható, a modularitása csekély, például a technikai és biztonsági kihívásoknak megfelelő módosítások – az úgynevezett szervizcsomagok – csak verejtékesen telepíthetők. Bár az NT-t felesleges lenne még temetnünk, látható hogy bizonyos szint fölé már nem lehet tovább fejleszteni.

A Windows 2000 megtervezése során már nem újabb felületcsinosítások, kisebb-nagyobb kényelmi funkciók bevezetése volt a Microsoft célja, hanem egyértelműen egy skálázható, stabil vállalati környezet megteremtése, akár a teljes korábbi rendszer újratervezésével. A befektetett több ezer emberévnyi fejlesztőmunka 2000 tavaszára hozta meg gyümölcsét, egy teljesen új, ámde a korábban megszokott, sikeres felület kényelmét nyújtó operációs rendszert.

Kiadványunk e heroikus munka eredményét mutatja be. Elsősorban nem Windows 2000 alaptanfolyamot próbálunk adni, hiszen a felület alapvető kezelése nem, vagy csak alig változott a Windows 98 óta. A Microsoft Magyarország és vezető hazai informatikai cégek Windows 2000 szakértőiből verbuválódott CHIPtár szerzőgárda számára nehezebben elérhető célt tűztünk ki, a Windows 2000 igazi mélységeinek közérthető feltárását. Mindazon dolgok bemutatását, amik nincsenek szem előtt, de egy korszerű vállalati informatikai rendszernek tudnia kell.

Azt, hogy siker koronázta-e igyekezetünket, elsősorban Kedves Olvasónk döntheti el. Reméljük, lapunk olvasgatása hasznos és érdekes időtöltésnek bizonyul!

Kiadványunk melléklete a Windows 2000 Útikalauz CD. A korong három hivatalos Microsoft Windows 2000 HTML tanfolyam magyar nyelvű változata mellett magyar és angol nyelvű műszaki tanulmányokat, multimédiás bemutatókat, valamint egy 250 oldalas magyar nyelvű kiértékelési útmutatót tartalmaz. Ez utóbbi átfogóan bemutatja mind a Professional, mind a Server változatok technikai újdonságait.

Tartalom

Windows 2000 – az új gazdaság alapja 6
A felhasználói termelékenység növelése 20
A Windows 2000 újításai a noteszgépes felhasználóknak 28
Megbízhatóság – felsőbb szinten 34
Automatikus szoftvertelepítés és karbantartás 42
Group Policy a Windows 2000-ben 46
A Windows 2000 fürtkezelése 50
A Microsoft Distributed File System (DFS) 53
Káosz és nyugalom – Életre hívott informatikai biztonság 58
A Windows 2000 biztonsági szolgáltatásai 63
Biztonságos honlap Certificate Serverrel 69
Hitelesség 2000 után Smart Card alkalmazásával 76
Lépcsőzetes frissítés a Windows 2000 rendszerre 80
Áttérés 82
Elosztott alkalmazások fejlesztése DNA 2000-ben 88

CHIPtár: Windows 2000

Felelős kiadó: Ivanov Péter • Szerkesztő: Kerecsen Tamás • Olvasószerkesztő: Nagy Anna • Címlapgrafika: Laza • Korrektor: Kovácsi Barnabás
Kiadja: Vogel Publishing Kft. 1139 Budapest, Hajdú u. 42–44. • Terjeszti: Hírlapkereskedelmi Rt. és a Nemzeti Hírlapkereskedelmi Rt. regionális részvénytársaságai. • Megrendelhető telefonon: (36-1) 349-4768-as vagy telefaxon a (36-1) 350-8731-es számon
Montírozás és nyomás: Veszprémi Nyomda Rt.
Copyright© „CHIP" Vogel Publishing Kft., Budapest, Magyarország • A közölt cikkek fordítása, utánnyomása, sokszorosítása, valamint adatrendszerekben való tárolása kizárólag a kiadó engedélyével történhet. A megjelentetett cikkeket szabadalmi vagy más védettségre való tekintet nélkül használjuk fel.
A Vogel Publishing Kft. a Magyar Terjesztés Ellenőrző Szövetség (MATESZ) tagja.

HU ISSN 1219-4522

A RENDSZER, AMELY MEGHALADJA KORÁT...

Cégfilozófiánk szerint teljes, működő rendszerek szállításával, komplex megoldások nyújtásával és az ezt támogató emelt szintű szervizszolgáltatási háttérrel lehet hosszútávon megbízható partnerré válni.

- **Teljes hardver és szoftver állomány részletes, rendszerszintű felmérése**
- **HW-SW rendszerek összehangolása, rendszerterv készítése**
- **Rendszerek leszállítása, telepítése és konfigurálása**
- **MCSE, MCP, CNE végzettségű szakemberek**
- **Tanácsadás (Partnereinknek térítésmentesen)**
- **CAT 5-ös és CAT 6-os hálózatok tervezése és kivitelezése ISO 9001 szerint**

Legkorszerűbb Activa számítógépeinket a Windows 2000 premierjével egyidejűleg már Windows 2000-rel szállítjuk, de felkészültünk arra is, hogy megvizsgáljuk a vállalatok jelenlegi gépparkját, tanácsot adjunk az átállással kapcsolatban, s ahol a helyzet erre érett, leszállítjuk és installáljuk a szükséges mennyiségben az új operációs rendszert. Szolgáltatási körünkbe beletartozik a tanácsadás és a konzultáció is, hiszen az új rendszerrel kapcsolatos ráfordítások csak annak térülnek meg, akik a Windows 2000 többlettudását ki is tudják használni.
Szakembereink az ország egész területén rendelkezésére állnak.
Keresse fel honlapunkat, és legyen partnerünk a minőségi számítástechnikában.

www.albacomp.hu

ALBACOMP

Microsoft Windows 2000

Albacomp Számítástechnikai Rt.

8000 Székesfehérvár Mártírok útja 9.
Tel.: *(22) 315-414, fax: (22) 327-532
www.albacomp.hu, e-mail: info@albacomp.hu

1139 Budapest Frangepán u. 8-10.
Tel.: (1) 350-8122
Fax: (1) 350-8325

Windows 2000 – az új gazdaság alapja

Horváth Tamás
tamash@microsoft.com

A Windows 2000 platform szerepére az információs társadalomban, illetve a magyar gazdaságban *Horváth Tamás*, a Microsoft Magyarország Windows termékmenedzsere mutat rá megvilágítva az operációs rendszer család szerepét a Microsoft vállalati termékskálájában, és bemutatva a technikai újdonságokat a négy fő tervezési cél mentén.

A számítástechnikai szaksajtóban az utóbbi években egyre gyakrabban találkozhattunk az „információs társadalom" kifejezéssel, ami arra utal, hogy a konvergáló technológiai piac – a számítástechnika, a távközlés és a szórakoztatóipar összeolvadása nem pusztán az új eszközök megjelentetésével és elterjesztésével lesz ránk hatással, hanem várhatóan a minőségi változás lehetőségét is megteremti a jelenlegi társadalomban.

Az informatikusok és a társadalomkutatók mellett az ezredév végére a közgazdászok is felismerték a változás jeleit. Az „új gazdaság" fogalmának megjelenése az ő szakterületükön is éreztette a minőségi változás előszelét, amely nem pusztán a technológia (és a technológiai cégek részvényeinek) gazdasági felértékelését hozta magával, hanem azt az általános szemléletet, mely szerint az új évezred üzletének középpontjában az információ, illetve annak gyors megszerzése és hatékony feldolgozása áll.

Az információszerzés leghatékonyabb formája ma az Internet, ezért tapasztaljuk napjainkban az internetes cégek tőzsdei mennybemenetelét. Elnyerték az üzleti élet szereplőinek bizalmát, ugyanis ők az „új gazdaság" működtetői.

A Microsoft a Windows 2000 platform megjelentetésével ezt az internetet szeretné átformálni a mindennapi hatékony munkavégzés céljából, és minden gazdasági szereplő számára üzletileg előnyösen felhasználhatóvá kívánja tenni. „Windows 2000 – The Business Internet starts here" – a Windows 2000 az Üzleti Internet kezdete, ahogyan azt a 2000. február 17-i amerikai termékbejelentésen *Bill Gates*, a vezető szoftvertechnológus hirdette.

Magyarországon?

Ez az internetes gazdaság azonban még távol van hazánktól. Vajon az információtechnológia újdonságainak van-e üzenete számunkra?

Az Internet, a globalizáció, valamint a felgyorsuló e-gazdaság elég távolinak tűnhet Magyarországon. Ha azonban jobban belegondolunk: mégsem az. Tavaly az ország GDP-jének 53 százaléka a multinacionális vállalatoktól származott. Ez azt jelenti, hogy hazánkban szinte bármely tetszőlegesen kiválasztott személy vagy éppen nemzetközi nagyvállalatnál dolgozik, vagy ha nem, akkor biztosan van a környezetében ilyen, s ennek a (munkadó) cége beszállítója vagy vásárlója.

A globalizációt tehát mi sem kerülhetjük el. A felgyorsuló gazdaság előszelét nálunk nem az Internet, hanem az uniós csatlakozás – az európai piaci liberalizációhoz való közeledés adja.

Felkészülő és belépő cégek

Hazánkban jelenleg két nagy vállalati kört különböztethetünk meg: az Internetre felkészülőket, illetve az arra kilépni szándékozókat. A kulcskérdés az első kör esetében a szemlélet kialakítása és a technológiai felzárkózás, míg a másodikéban a technológia szervezeti és üzleti integrálása. Mindkét esetben stratégiai váltás szükséges, ugyanis szembe kell nézni a kihíváa-

sokkal: az „új gazdaság" szabályait meg kell érteni és elfogadni azokat.

Ezek a gondolatok vezéreltek bennünket a Microsoft Magyarországnál, amikor megalkottuk a Windows 2000 hazai üzenetét – a Windows 2000-es információtechnológiát. Hazánkban szintén az üzleti gondolkodás részévé lehet tenni, felkészítve így a cégeket az Internetalapú piaci működésre, ezért méltán nevezhetjük a változások kiváltójának és „az új gazdaság alapjának".

Felkészülés és belépés az új gazdaságba

Az első körbe tartozó vállalatok esetében a felkészülés lépései világosan láthatók, hiszen számos cég járta már végig ezt az utat, amellyel követendő példát mutatott. A PC-s munkahelyek megteremtése a kezdet a hatékony munkavégzéshez, ezt a hálózat kiépítése, majd a papíralapú kommunikáció elektronikus formával történő kiváltása követi.

A következő fontos állomás a belső elektronikus levelezés elindulása, továbbá elengedhetetlen a könyvelési és ügyviteli rendszer számítógépesítése, valamint a kulcsfontosságú üzleti folyamatok elektronikus kezelése. A folyamat végére a teljes vállalat működése egyetlen integrált informatikai rendszerbe kerül, a belső ügyek rendezése után pedig ki lehet tekinteni az internet felé.

A következő lépés az internetes, külső levelezés feltételeinek megteremtése, majd a külső megjelenés saját weboldallal – ezt követi a belső intranet kialakítása, majd miután a teljes vállalat webtechnológiát használ, a beszállítói láncbeli partnerekre is ki kell ezt terjeszteni. Mihelyt az üzletközi tranzakciók is elektronikusan zajlanak, jöhet a végső lépés: az Interneten keresztül e-kereskedelmi weboldal segítségével történő kapcsolatfelvétel a fogyasztókkal.

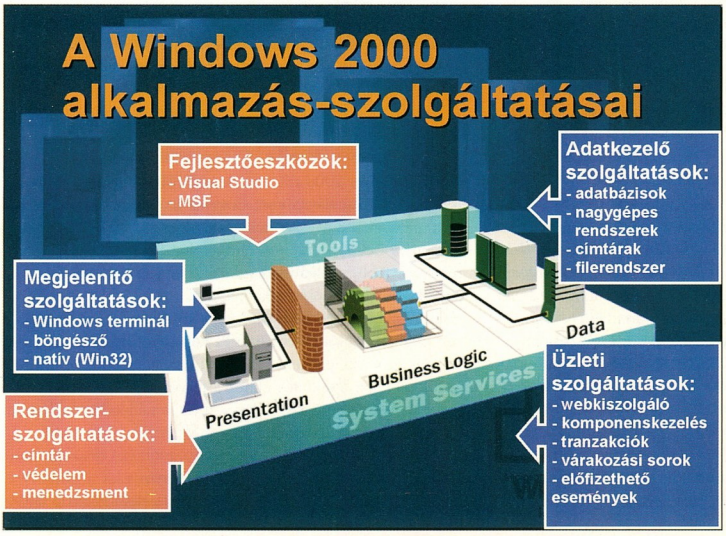
Szervezet és technológia

Hogyan teremti meg a fenti lehetőségeket a Windows 2000 és a Microsoft? A kérdés megválaszolásához általános vállalati modellt mutatok be: tetszőleges gazdasági szervezet üzleti–kommunikációs folyamatait e szerint az alábbi típusokra oszthatjuk fel:

- szervezeten belüli (**intra-business** vagy **business-to-enterprise**);
- szervezetek közötti (**business-to-business**)
- a szervezet és ügyfelei közötti (**business-to-consumer**) kommunikáció.

A kommunikáció mindhárom csoportban felbontható strukturált és strukturálatlan (avagy formális és informális) részekre. Strukturált kommunikáción és folyamatokon itt a törvényi rendeletek, a gazdasági szabályozások és az előírások, a szabványok, a belső szervezeti és működési szabályzatok által meghatározott formájú, „hivatalos" adat- és információcserét értem, míg a strukturálatlan rész a szabályozatlan, az esetleges, illetve a kötetlen (az üzleti folyamatok szempontjából azonban ugyanolyan fontos) kommunikációt takarja.

Jelenleg a szervezetek legnagyobb gondját az okozza, hogy a különböző típusú üzleti folyamataik kezelése más-más szervezeti egységeik felügyelete alatt van, a fenti kommunikációs típusokhoz használt technológiák pedig egyediek és egymástól különbözőek, így az eltérő koncepciók következtében az együttműködésük nehézkes. Mindez gátolja a szervezet hatékony munkavégzését.



A megoldást olyan egységesített háttér kínálja, amely összefüggő rendszerben kezeli mindhárom kommunikációs típust, és a technológiai megvalósítás során egyaránt figyelembe veszi az üzleti folyamatokat és a fellépő igényeket.

A Microsoft víziója a fenti egységes koncepció alapján működő szervezet megvalósítását szolgáló digitális idegrendszer.

Ez olyan vállalati modell, amely üzleti szemszögből közelíti meg a szervezet felépíté-

sét, és ehhez a képhez illeszti a gazdasági folyamatokat segítő információ technológiát. A Microsoft célkitűzése, hogy minden egyes vállalati terméke alkalmazkodjon ehhez a modellhez, így a technológiailag integrált megoldások üzleti szinten is egységes koncepcióba illeszkedjenek.

A digitális idegrendszer modelljében a szervezet három meghatározó alkotórészre bontható:

- **Emberek**: a szervezet statikus építőelemei.
- **Folyamatok**: a szervezet működését, a tagok egymás közötti interakcióját meghatározó erők és mozgások rendszere.
- **Partnerek**: a szervezet környezete, a külvilág. Az üzleti partnerek, más szervezetek, és a szervezet által kiszolgált ügyfelek is ide tartoznak.

Emberek – ismeretkezelés

Az úgynevezett ismeretkezelés, avagy knowledge management az emberek közötti hatékony kommunikációt elősegítő informatikai módszer. Ennek fegyvertára kiterjed mind a formális, strukturált információcserére, mind az informális adatáramlás elősegítésére. Előbbi a hivatalos űrlapok, rögzített mezőkkel bíró iratok kezelését oldja meg akár az elektronikus levelezőrendszerekkel együttműködve, vagy pedig belső vállalati intranet oldalak segítségével. A strukturált kommunikációhoz még az úgynevezett workflow, az emberek kommunikáció-cseréjének folyamatát, dinamizmusát leíró szabályok kezelése és modellezése tartozik.

Az informális kommunikációt rengeteg eszközzel elősegíthetjük, kezdve az egyszerű elektronikus levelezéstől, a faliújságokon, a nyilvános fórumokon, a valós idejű csevegő fórumokon, a videokonferenciákon, a multimédia oktatóanyagokon keresztül egészen a webalapú intranetre való egyszerű publikálásig, vagy a levelezőrendszerbe ágyazott dokumentum-megosztási képességekig. Ezeknek a használata azonban csak akkor hatékony, ha szervezeti szabályzatok, ajánlások rögzítik a fontosabb irányelveket.

Microsoft Office + Exchange = ismeretkezelő platform

A Microsoft Office 2000 alkalmazáscsomag központi eleme az Outlook 2000, mely a többi irodai alkalmazást (Word 2000, Excel 2000, Powerpoint 2000, Access 2000, Frontpage 2000) fogja össze, és teszi csoportmunkára alkalmassá. Az Outlook 2000 nem egyszerű levelezőprogram, hanem – a Microsoft szóhasználatában – „ismeretkezelő portál", központi felület, kapu, amelyen keresztül az összes csoportmunka-szolgáltatás elérhető a rendszerben. Az ismeretkezelés hátterét az Exchange kiszolgáló adja.

Üzleti folyamatok – üzleti alkalmazások

A belső, vállalati működés szabályai, az üzleti folyamatok jelentik a cégek legfontosabb értékét, ezeket a folyamatokat egyrészt állandóan gyorsabbá és hatékonyabbá kell tenni, másrészt rugalmasan át kell alakítani a változó piaci körülmények hatására. Az egyes részterületek (könyvelés, ügyvitel, pénzügy, raktározás, termelés, kereskedelem, marketing, személyzeti politika) kezelését össze kell hangolni a közös vállalati cél érdekében. Erre a feladatra a cégek már évek óta szakosodott, a vállalati működés minden területét lefedő integrált vállalatirányítási informatikai rendszereket használnak.

A Microsoft azonban nem kíván belépni a vállalatirányítási rendszerek piacára. A digitális idegrendszer egyrészt alkalmazás-kiszolgáló infrastruktúrát kínál ezeknek a rendszereknek (a legnagyobb gyártók, az SAP, Baan, Peoplesoft, JDEdwards, Scala mind a Microsoft stratégiai partnerei), másrészt a Visual Studio fejlesztőkörnyezet fejlesztési platformot ad a – kiadványunkban részletesebben is ismertetett – Windows DNA fejlesztési modell segítségével az egyedi célú üzleti alkalmazások gyors és költséghatékony elkészítéséhez.

Elektronikus kereskedelem

A fentiekből látszik, hogy az elektronikus kereskedelem csak része az e-üzletnek, a vállalatot átszövő informatikának, digitális idegrendszernek. A partnerekkel történő B2B üzleti kommunikációt, valamint a beszállítói lánc kezelését az internetes szabványra, a webalapú XML-re épülő BizTalk protokoll teszi hatékonnyá az üzleti adatformátumok szabványosításával. A Windows DNA fejlesztési modell kifejezetten a webes elektronikus kereskedelmi alkalmazások támogatására optimalizált.

A fogyasztót megcélzó, B2C webáruházak kialakításához és működtetéséhez a Microsoft Commerce Server ad keretrendszert, mely automatikusan lekezeli az áruházak üzleti folyamatait (árazás, adózás, promóciók, marketing adatbázis, fogyasztói profilok készítése, vásárlói szokások mérése, logisztika stb.)

Mi a Windows 2000 szerepe a digitális idegrendszerben?

A Windows 2000-ről mint termékről eddig nem esett szó. Az alapgondolatunk az volt, hogy az üzleti kommunikációt és alkalmazásokat egységes üzleti szemléletbe kell ötvöznünk – a Windows 2000 operációs rendszer család infrastruktúrát teremtve a többi szolgáltatás számára adja ennek az egységnek az informatikai alapját, a közös platformot. A rendszer felépítését az alapozással kell kezdeni, ezért fontos a jól megtervezett, átgondolt Windows 2000-es környezet bevezetése, amire később sorra építeni lehet az üzleti szolgáltatásokat. A következő technikai áttekintés ehhez a tervezéshez és építkezéshez nyújt segítséget, így a Windows 2000 remélhetően valóban az új üzlet, az új gazdaság alapja lesz.

A Windows 2000 céljai a tervezés során

A Windows 2000 technikai tervezési céljait négy fő terület köré csoportosíthatjuk, bár a rendszer integrált volta következ-

tében az egyes területek technológiái között átfedés van. Ezek a tervezési célok az alábbiak:

- **A megbízhatóság és a skálázhatóság növelése** a biztonságos nagyvállalati alkalmazás-kiszolgáló és e-üzlet platform megteremtése céljából.
- Hatékony és egyszerű **rendszermenedzsment, valamint -felügyelet** az üzemeltetési költségek csökkentésére.
- Integrált, minden alkalmazás számára elérhető, magas színvonalú **infrastrukturális szolgáltatások**.
- **Alkalmazásplatform** szolgáltatások az üzleti alkalmazások fejlesztésére, futtatására és karbantartására.

Tekintsük át a Windows 2000 technikai újdonságait e tervezési célok tükrében.

Megbízhatóság

Valamely új operációs rendszer vállalati bevezetésekor az a legfontosabb szempont, hogy mennyire megbízható és az alkalmazások mennyire biztonságosan futnak rajta. A Windows 2000 a biztonságos, védett alkalmazás-memóriaterületű Windows NT architektúrára épül, azonban a kernel további fejlesztései tovább növelték a stabilitását.

Kevesebb újraindítás: az újraindítások száma erőteljesen mérséklődött – több mint 70 olyan esetet kiküszöböltek, melyekben korábban a rendszerkonfiguráció átállítása miatt újraindításra volt szükség – jelenleg hét konfigurációs kategória maradt csak, amely újraindítást igényel (például a processzor- és memóriacsere is közöttük szerepel). A leállások a plug and play támogatásnak köszönhetően is csökkentek. Ez most először került bele a Windows NT vonalba – a laptop gépeken ez a szolgáltatás igazán látványos és kényelmes a PCMCIA kártyák működés közbeni cseréjekor.

„Önjavító" tulajdonságok: további újdonság, hogy ha az alkalmazások konfigurációja megsérül, a rendszer önmagától képes helyreállítani az eredeti beállításokat és környezetet a Windows Installer segítségével. Ez a rendszerszolgáltatás végre megoldja az alkalmazások életciklusának teljes körű felügyeletét a telepítési, a karbantartási és az eltávolítási szakaszokra kiterjedően – mivel a Windows Installer az operációs rendszer része, nyilvántartja az összes telepített alkalmazást,

így a felügyeletük megbízhatóbb lesz, hiszen az nem az alkalmazás által generált (vagy nem generált) install és uninstall szövegállományoktól függ (melyek korábban általában legelsőként estek áldozatul a felhasználók lemezterület-felszabadítási akcióinak).

A Windows 2000 a különböző verziójú DLL-ek által okozott gondokra és a közösen használt, más verziójú DLL-ek felügyeletére is ad megoldást: a más alkalmazás által átírt vagy letörölt korábbi (vagy későbbi) verziójú DLL-ek az úgynevezett DLL cache-ből, vagy a Windows Installer szolgáltatással az eredeti telepítési pontról automatikusan helyreállíthatók.

A System File Protection szolgáltatás ugyanígy állítja helyre automatikusan a letörölt rendszerállományokat is.

Service Pack „slipstreaming“: a szoftverek élete ma folyamatos fejlődésből áll, az operációs rendszerekre ez kétszeresen is igaz: a finomítások és hibajavítások eredménye a Microsoft termékek esetében a Service Pack, vagyis szervizcsomag. Ilyet természetesen a Windows 2000-re is kibocsátanak, hiszen a kód evolúciója nem áll meg a kiadás napján. A szervizcsomagok kezelése viszont sokkal könnyebbé vált, mert az eredeti kóddal egybevonhatók, így készíthető olyan telepítő készlet, amely rögtön az aktuális szervizcsomagú változatot telepíti fel. Így nem kell utólag (és a szolgáltatások újratelepítése után) újra és újra feltenni a Service Pack változatokat.

Meghajtó-hitelesítés (driver signing): a tapasztalatok szerint a legtöbb rendszerleállást és meghibásodást a kernel módban működő, külső gyártótól származó rosszul megírt szervizek, illetve meghajtóprogramok okozzák. Ekkor nincs lehetőség szigorú memóriavédelemre, a meghajtószoftvernek közvetlen hozzáférést kell adni a hardverhez, az egyéb kernelszintű összetevő egymástól való további védelme ugyanis lassítaná a rendszer működését. A Microsoft a Windows 2000 esetén kéményen megszigorította a külső összetevők fejlesztési előírásait, és az ezeknek megfelelő meghajtóprogramokat, valamint az egyéb szoftverkomponenseket digitális aláírással látja el.

A driverek hitelessége (aláírása) ellenőrizhető a rendszerből, így a gyanús összetevők könnyen azonosíthatók hiba esetén. Természetesen általában a hiba csak úgy hárítható el, ha megfelelő (a *Hardver-kompatibilitási Listán* szereplő) hardvereszközre váltunk.

Skálázhatóság

A platformok méretezhetősége szintén kritikus szempont a vállalati bevezetés mérlegelése során. A Windows 2000 szolgáltatásai egyrészt tetszőleges méretű vállalkozásokat kell, hogy kiszolgáljanak, másrészt a vállalat méretének növekedésével a platformnak is nagyobb teljesítményt kell nyújtani, hiszen a platformváltás költségesebb, mint a szoftver alatti hardvereszközök bővítése.

A Windows 2000 a növekvő teljesítményt egyrészt a felfelé skálázással, az egyre nagyobb, több processzoros és több memóriával bíró gépek használatával, másrészt az oldalra skálázással, az egyre több, azonos szolgáltatást nyújtó gép beállításával növeli.

Háromrétegű alkalmazások méretezése: a nagy rendelkezésre állás és a jó skálázhatóság kulcsa a többrétegű alkalmazásfejlesztésben rejlik. A Windows 2000 alkalmazásfejlesztési modellje, a Windows DNA (Distributed Network Architecture) három alkalmazásréteget különböztet meg: a megjelenítési, az üzleti logika és az adatbázis rétegeket (ezeket front-end, middleware és back-end rétegekként is emlegetjük.) A Windows 2000 különböző skálázási, fürtözési technológiákat teremt az egyes alkalmazásrétegek számára.

Hálózati terhelésmegosztás (NLBS – Network Load Balancing): a front-end rétegben a megjelenítést végző ügyfelek csatlakoznak az üzleti folyamatokat modellező középső réteg kiszolgálóihoz. Ez a kapcsolat lehet webböngésző és webszerver kapcsolata, de akár 32 bites „vastag“ ügyfélprogram és szerveroldali párjának kapcsolata. A Windows 2000 a középső réteg kiszolgálói oldalán az IP-protokoll felett nyújtott bármilyen statikus szolgáltatást (http, ftp, terminálszolgáltatás stb.) képes elosztani maximum 32 gép között, így az ügyfelek terhelése egyenletesen terül szét a kiszolgálókon jobban kihasználva

Néhány érdekes adat

- Több mint 5000 ember vett részt a Windows 2000 fejlesztési projektben.
- A Windows 2000 csapat nemzetközi fejlesztőinek száma több mint 1500.
- A Windows 2000 operációs rendszert a megjelenés napján már körülbelül 700 ezren használták.
- 11 500 hardvereszköz működik együtt a Windows 2000-rel.
- Az Egyesült Államokban összesen 1608 vállalat vett részt a Windows 2000 megjelenés előtt kiértékelésében.
- A 2000. február 17-i kiadásig több mint 120 ezer szakember vett részt Windows 2000 oktatáson.
- A Windows 2000-hez már kb. 7000 alkalmazás érhető el és havonta további 500 új alkalmazás jelenik meg.
- A Windows 2000 Professional 23 nyelven lesz elérhető.
- A Windows 2000 Server 17 nyelven kapható majd, ez lesz az első, teljesen honosított magyar kiszolgálótermék.
- A Windows 2000 fejlesztését 50 ország 300 ezer telephelyén, 23 nyelven, 130 különböző nyelvjárást beszélő emberek végezték.
- A Windows 2000 projekt tagjai naponta 90 ezer e-mailt küldtek egymásnak.
- A Windows 2000 platform TPC-C adatbázis benchmark rekordot döntött megjelenése napján: a 12 kiszolgálós, 8 utas Compaq ProLiant fürtben Windows 2000 Advanced Serveren futó SQL Server 2000 eredménye: 227 TPC, ez 63%-kal magasabb, mint a korábbi 135-ös rekord.

azok kapacitását. Ezt a megoldást hívjuk kiszolgálófarmnak – a farmot működtető NLBS szolgáltatás a Windows 2000 Advanced Servertől kezdve elérhető a Windows 2000 Server családban. Előnye, hogy újabb kiszolgáló beállításával a teljesítmény a szolgáltatás leállítása nélkül, egyszerűen, lineárisan növelhető, egy-egy kiszolgáló kiesése esetén pedig a farm szolgáltatása (mérsékelt teljesítménnyel) továbbra is elérhető marad. A farmok szolgáltatása még az úgynevezett rolling update funkció, mely a kiszolgáló szoftver frissítését szintén szolgáltatás-kiesés nélkül valósítja meg: a frissítendő kiszolgálókat egyenként lekapcsolja, frissíti, majd visszaállítja. (A fürtözésről és a terheléselosztásról további részletek olvashatók *A Windows 2000 fürtkezelése* című cikkünkben.)

Komponens-terhelésmegosztás (CLBS – Component Load Balancing): a középső réteg, a middleware tartalmazza az üzleti folyamatok modelljét, az alkalmazáslogikát. Az üzleti logika alkalmazásait célszerű a komponenstechnológiát kihasználva elkülönített részekre bontani, hiszen az így keletkezett önálló alkalmazás-összetevők futtatása helyileg szétosztható legfeljebb nyolc, egyenletesen terhelt kiszolgáló között. Ha a vállalat nagyobb teljesítményt kíván, ez további kiszolgálók beállításával és az összetevők átcsoportosításával egyszerűen megtehető – az ügyfél számára a CLBS-farm egyetlen szolgáltatásként jelenik meg.

Lineárisan méretezhető kiszolgálófarm-felügyelet az AppCenter Serverrel: a fent bemutatott CLBS különálló, Windows 2000-alapú kiszolgálótermékben, az AppCenter Serverben érhető csak el. Láttuk, hogy a kiszolgálófarmok teljesítménye mind a hálózati, mind az összetevő-terhelésmegosztással lineárisan nő – a farmban található kiszolgálók felügyelete viszont a növekedéssel egyre bonyolultabb és nehézkesebb lesz. Az AppCenter Server feladata megteremteni a kiszolgálószámtól független, egységes kiszolgálófarm-felügyeletet, mely ugyanolyan egyszerű 32 szerver esetén is, mint a kétgépes farmon.

Kiszolgáló fürtözés (clustering): a háttérben, az adatbázis rétegben nem is annyira a méretezhetőség, mint inkább a nagy rendelkezésre állás a fontosabb az üzleti adatok védelme céljából. A Windows 2000 Advanced Server maximum két kiszolgálóból álló hibatűrő fürtöt tud alkotni, míg a Windows 2000 Datacenter Server négy csomópontos hibatűrő fürt kezelésére képes. A fürtök csomópontjai itt „forrótartalékként" működnek, azonnal észreveszik az aktív csomópont kiesését, és automatikusan átveszik annak szerepét.

Rendszermenedzsment és -felügyelet

Egyre több vállalat ismeri fel napjainkban, hogy az informatikai rendszerek teljes bekerülési költségeinek a szoftver- és a hardvereszközök beszerzési költségei csak kis hányadát teszik ki – az élettartamra vetített költségek túlnyomó részét az oktatási, rendszerüzemeltetési és karbantartási költségek teszik ki. A Gartner Group referenciának számító tulajdonlási költségelemzése szerint (TCO – Total Cost of Ownership) a szoftver és hardver pusztán egyharmadát teszi ki a teljes költségeknek.

Ennek egyik mérséklési módja a hatékony rendszerfelügyelet, amely a Windows 2000 tervezésekor is központi szerepet kapott mind a munkaállomás (Professional), mind pedig a kiszolgálócsalád változataiban.

A kitűzött cél egyszerűen megfogalmazható: a Windows 2000-et futtató számítógépek menedzsmentje legyen jóval egyszerűbb, az egy számítógépre fordított menedzsment idő csökkenjen, és ezzel a napi üzemeltetés költsége is mérséklődjön. Ezzel egy időben viszont a végfelhasználó munkájának hatékonysága növekedjen.

A fenti célt kielégítő Windows 2000-es felügyeleti szolgáltatások három részre oszthatók:

- központi (címtáron alapuló),
- távoli és
- alkalmazás-felügyeleti megoldásokra.

Az IntelliMirror: az elgondolás a Windows 2000 felügyeleti felépítésének központi gondolata. Az IntelliMirror nem szoftver, nem is technológia, hanem ama rendszerfilozófia megnevezése, amelyet többfajta, különálló szolgáltatás valósít meg. Az IntelliMirrort használva a vállalati felhasználó bárhol, bármely gépen dolgozhat a hálózaton (vagy attól távol), mindig ugyanazt a munkakörnyezetet fogja kapni. Egész pontosan az IntelliMirror biztosítja a felhasználónak, hogy ahová megy, oda

- a dokumentumai,
- a beállításai,
- és az alkalmazásai kövessék.

Kövessenek a dokumentumok! – Offline mappák: az úgynevezett offline mappa a Windows 2000 Professional újdonsága. Használata a régi *Briefcase-éhez (a Táskához)* hasonlít, ám annál nagyságrendekkel kényelmesebb és praktikusabb. A Professionalben bármely hálózati mappához, vagy a benne található állományhoz megadhatjuk, hogy offline módon is szeretnénk elérni – ekkor a munkaállomás automatikusan másolatot készít az állományból a helyi lemezre. Ezt szintén automatikusan szinkronizálja, ha a hálózati (vagy helyi) állomány tartalma változik. Ez a szolgáltatás a noteszgépek esetén akkor kényelmes, amikor a hálózattól távol ugyanazt a kiszolgálónevet és útvonalat megadva elérjük a hálózati állományokat, mintha csak a cégnél dolgoznánk, vagyis a felület átlátszó a felhasználó számára, nem számít, hogy a másolatot, vagy a hálózati példányt használja-e. (Erről a technológiáról további részletek *A felhasználói termelékenység növelése* című cikkben olvashatók.) Az offline mappák hatékony felhasználására példa a vállalati munkaállomások *My Documents (Dokumentumok)* mappáinak „átirányítása" a kiszolgálóra. A felhasználók a saját gépükön hoznak létre dokumentumokat a megszokott mappájukban a helyi lemez elérési sebességével (nem kell a lassú hálózati „home" könyvtárakra várni). A helyi példány azonban

folyamatosan szinkronizálódik a kiszolgálón lévő másolattal, így a felhasználó a dokumentumait egyrészt minden gépről látja, másrészt másolat automatikusan készül róla, és onnan pótolható, ha a merevlemez véletlenül tönkremenne. A sok-sok helyi szalagos mentés, vagy írott CD-archívum készítése helyett így a rendszergazdának csak a kiszolgálót kell mentenie központi helyen.

Kövessenek a beállítások! – Active Directory Csoportos Házirend (Group Policy): a házirend (policy) alapú felhasználói felügyelet már a Windows NT 4.0-ból ismerős lehet – abban szinte csak tiltásokat és korlátozásokat adhattunk meg a házirenddel, és az a tartomány szintjén jutott érvényre. A Windows 2000 Csoportos Házirendje (melyről kiadványunkban részletesebben is olvashatnak a *Group Policy a Windows 2000-ben* cím alatt) azonban inkább a szabványos felhasználói környezetek kialakítására és menedzsmentcélokra használható, kevésbé korlátozódik csak a tiltások és korlátozások szintjére. A Csoportos Házirend az Active Directory címtár hierarchikusságának köszönhetően több szinten is alkalmazható, így nagyobb rugalmasságot enged.

A Csoportos Házirendekkel megadhatók

- a felhasználók (helyesebben bármilyen címtárbeli objektum) registry beállításai,
- a biztonsági beállítások,
- a szoftvertelepítés adatai, továbbá
- a kiemelt mappák átirányíthatók és
- többszintű scriptelés valósítható meg, azaz a logon/logoff parancsállományok is a címtárban, és nem a file-rendszerben tárolódnak.

Kövessenek az alkalmazások! – Windows Installer:

A Windows Installer talán a legjobban kihasználható újítás a Windows 2000-ben, amely a rendszergazdákat megszabadíthatja számos rutinmunkától. Fontos kiemelni, hogy a Windows Installer nem kötődik a Windows 2000-hez, hiszen NT 4.0-n és a Windows 9x platformon is létezik, és kernel módú szolgáltatás formájában használható.

A Windows Installer tranzakció-alapú telepítő szolgáltatás, amely az alkalmazás teljes életciklusát felügyeli az installálási, a karbantartási, valamint az eltávolítási folyamatok egységes, rendszerszolgáltatásként nyújtott kezelésével. A Windows Installer nemcsak a telepítő készletet, hanem a telepítési műveleteket, az adatformátumokat és a függőségeket is meghatározza és nyilvántartja.

Használatával a felhasználóknak „meghirdethetünk" alkalmazásokat, amelyeket igény szerint telepíthetnek, vagy hozzájuk rendelhetünk szoftvereket, melyek ugyan megjelennek a Start menüben, de csak az első hozzáférés, illetve futtatás folyamán települnek fel a rendszerre.

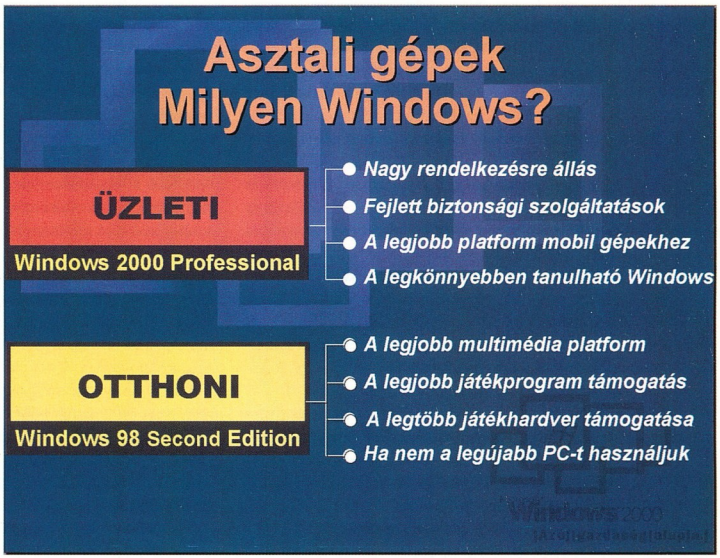
A Windows Installer adott alkalmazás futtatása előtt ellenőrzi a szükséges összetevők épségét és meglétét, hiba esetén pedig az eredeti telepítési pontról (CD-ről vagy hálózati megosztásról) automatikusan javítja az adott elemet felhasználói beavatkozás nélkül.

Az automatikus telepítésszolgáltatással az eredeti telepítő készletünkből egyedi, testre szabott telepítő változatokat készíthetünk az úgynevezett transzform file-ok segítségével.

A tökéletes, operációs rendszer szinten felügyelt alkalmazás-eltávolítás a „DLL-pokol" galibáit küszöböli ki az osztottan használt összetevők intelligens kezelésével. (Ezt a szolgáltatást alaposabban az *Automatikus szoftvertelepítés és karbantartás* című cikkben ismertetjük.)

Nyelvi támogatás (Multiuser interface – MUI):

A többnyelvű vállalati környezetekben a különböző nyelvi változatú operációs rendszerek és alkalmazások felügyelete mindig gondot jelent – általában a Service Packek és hotfixek esetében, amelyek eddig egyediek volt a nyelvi változatok szempontjából. Az úgynevezett multiuser interfész megjelené-



sével a programkód függetlenedik a nyelvi felülettől, az utóbbi tetszőlegesen változtatható akár felhasználónként is, azaz ugyanazon a gépen az angol felhasználó angol, a magyar pedig magyar nyelvű felületet kaphat automatikusan a bejelentkezés után. Mivel a MUI alatt lévő kód azonos, az oprendszer és alkalmazás-felügyelet egységes az összes nyelvre (már az Office 2000-nek is van MUI változata).

Infrastrukturális szolgáltatások

Az infrastrukturális szolgáltatások közé azokat a rendszerfunkciókat soroljuk, amelyeknek mindenütt, az összes felhasználó és valamennyi alkalmazás számára elérhetőnek kell lenniük. Fontos, hogy ezeket a szolgáltatásokat a platform egységesen adja, ne az alkalmazások fejlesztőinek, a külső eszközök gyártóinak kelljen egyedi, egymástól eltérő és ezért nem kompatibilis megoldásokat készíteniük.

Az infrastruktúrát a Windows 2000 esetében négy területre érdemes bontanunk:

- központi címtárszolgáltatások az Active Directory segítségével;
- file- és nyomtatószolgáltatások;
- hálózati szolgáltatások;
- biztonsági szolgáltatások.

Címtárszolgáltatások: a Windows 2000-es infrastruktúra alapja az Active Directory címtárszolgáltatás, mely olyan elosztott rendszer, amelyik a hálózati erőforrásaink adatait egyetlen központi helyen tárolja.

Ezek az erőforrások tetszőlegesek lehetnek: a már megszokott, címtárban tárolt felhasználói adatok, a munkaállomások adatai és a kiszolgálók szolgáltatás-elérési pontjai (megosztások, házirendek stb.) mellett a hálózati eszközök, a tűzfalak, a levelező rendszerek, az üzleti alkalmazások és más címtárak adatai is itt tárolhatók.

A Cisco eszközök Active Directory integrációja segítségével például megadhatjuk azt, hogy ha az igazgatónk használja az SAP/R3 ügyfélprogramját, akkor a cég két távoli telephelyét összekötő routerek automatikusan lefoglaljanak egy adott sávszélességet erre a kommunikációra, így a többi felhasználó adatforgalma semmiképp sem lassítja a kapcsolatot.

Hierarchia: az Active Directory Services (AD, vagy ADS) a Windows NT 4.0 NTDS címtárszolgáltatását váltja fel, amit népszerűbb nevén domain vagy tartományi modellnek hívtunk. Az Active Directory szintén ezekre a tartományokra épít, azonban a tartományok és az erőforrások itt hierarchikus rendbe, fastruktúrába vannak csoportosítva. A hierarchia kialakításának több szempontja is lehet – ennek nem feltétlenül a szervezeti felépítés hierarchiájának tükrözésének, illetve a leképezésének kell lennie. A faszerkezet tervezése során inkább a hálózati kapcsolatok sebességét és a földrajzi elhelyezkedést kell figyelembe venni. Az AD képes a fastruktúra több nézetből történő megjelenítésére, hiszen a rendszergazda szempontjából például az azonos jogosultságú embereknek kell egy csoportba kerülniük, míg a felhasználó a vállalati hierarchia alapján a főnök–beosztotti viszonyokra kíváncsi, ami pedig két teljesen eltérő rendező elv.

Bővíthető séma: az Active Directory nagy előnye, hogy tetszőlegesen bővíthető újabb objektumokkal és tulajdonságokkal (az ún. séma bővítésével), ezeket aztán a rendszer ugyanúgy kezeli, mint a beépített tulajdonságokat. Hasonlatként képzeljük el, hogy az egyik állományrendszerben az állományokat leíró tulajdonságokat – a létrehozás dátuma, a méret, a tulajdonos, a jogosultságok mellett – valamilyen egyéni tulajdonsággal szeretnénk bővíteni; például olyan szín tulajdonsággal, amely azt írja le, hogy az állomány létrehozója milyen színű sapkát viselt. Ezt a tulajdonságot egyszer kell értelmezni, és utána minden állományra meghatározható és lekérdezhető lesz (pl.: a dir paranccsal), mintha mindig is az állományrendszer része lett volna. Az Active Directory objektumai ugyanígy bővíthetők – adott felhasználó adatai mellé odatehetjük például a fényképét, az anyanyelvét, a költségkeretét, a szobája számát, ezek az adatok így mindenki számára egy helyen lesznek elérhetők.

Programozási felület: az Active Directory teljes körű vállalati kihasználhatóságának kulcsa az, hogy nyílt programozási felülete van. Az ADSI (Active Directory Services Interface) lehetővé teszi, hogy az általunk fejlesztett alkalmazásokat integráljuk a címtárral, legyen szó akár Visual C-ben, C++-ban megírt, de akár az egyéb környezetben fejlesztett alkalmazásokról. Az ADSI Visual Basicben és más egyszerű scriptnyelven is használható, így a címtárműveletek végrehajtásához a rendszergazdának nincs szüksége fejlesztői tapasztalatokra, a megszokott script környezetében dolgozhat (ezt a Windows Scripting Host segítségével a Windows 2000-en tetszőlegesen választhat, akár unixos awk, perl, akár RexX, vagy más ismert scriptnyelvek közül is). Természetesen nem szabad megfeledkezni arról sem, hogy az Active Directory az Interneten szabványos LDAP protokollon keresztül is elérhető.

Áttérés és együttműködés: az Active Directory a Windows 2000 platform lelke – a vállalaton belül azonban az összes információ áttétele erre a központi címtárszolgáltatásra meglehetősen sok időt vesz igénybe és gondos előzetes tervezést feltételez. Éppen ennek a következményeként a Microsoft a lehető legtöbb eszközzel támogatja a folyamatos áttérést a korábbi Windows NT 4.0 domainmodellről, illetve más címtárszolgáltatásokról. A 4.0-s tartományok és az Active Directory egyszerre jelen lehetnek egyazon hálózaton az úgynevezett vegyes működési módban (Mixed mode). Ekkor a régi címtár még használható azokra a funkciókra, amelyek átállítása még nem történt meg, azonban az Active Directory számos új szolgáltatása is elérhető lesz már. Más gyártók címtárairól (Lotus Notes, Netscape Directory Services, NIS+, unixos LDAP-alapú címtárak vagy akár a Novell NDS) az együtt létezést és az áttérést a szinkronizációs eszközök, az úgynevezett konnek-

torok valósítják meg, melyek folyamatosan összhangban tartják azokat a felhasználói és egyéb erőforrásadatokat, amelyek mindkét címtárban szerepelnek. (Az áttérés lépéseit az *Áttérés* című cikkünk mutatja be.)

Nagyvállalati környezetben a heterogén címtárkörnyezet egységesítése túl nagy költséggel járhat – számukra a legjobb megoldás a meglévő, több gyártótól származó címtárak központosítása, egységes üzleti logikába és felügyeletbe kapcsolása a Microsoft Metacímtár-szolgáltatás (MMS – Microsoft Metadirectory Services, a korábbi ZoomIt nevű cég VIA terméke) segítségével.

File- és nyomtató szolgáltatások: a Windows 2000 a hagyományos file- és nyomtató-kiszolgálás területén is számos újdonságot hoz, melyek elsősorban a rendelkezésre állást és az adatbiztonságot növelik. Így az NTFS5 például megvalósítja a lemezkvóták kezelését, titkosítást nyújt az adattárolás szintjén (így a merevlemez fizikai eltávolítása esetén sem férhetnek adatainkhoz), beépített töredezettség-mentesítést tartalmaz, és a parancsikonok már követni tudják az időközben más könyvtárakba, vagy akár másik kiszolgálóra mozgatott állományokat a Distributed Link Tracking segítségével. A file-rendszer intelligensen bővíthető tulajdonságokkal, és kötetek csatolhatók hozzá dinamikusan működés közben (a Unixból ismerős mount eljárással). A rendszer szolgáltatásaként a kötetek működés közben dinamikusan átméretezhetők, nem kell tovább harmadik gyártó eszközét (pl.: Partition Magic) használni erre a célra. A skálázhatóságra példa az eddigi legnagyobb, 2,18 TB-os NTFS5-ben tárolt file, amelynek létrehozása 18 órán át tartott...

Az Indexszolgáltatás a Professional munkaállomáson és a kiszolgálón is elérhető; ez teljes szöveges keresést valósít meg a dokumentumokon, tulajdonságaikon, legyenek azok a saját gépen, weben vagy a hálózat tetszőleges helyén. A keresési teljesítményt ezúttal az előzetes indexelés teremti meg – érdekesség, hogy a Morphologic Kft. már elkészítette az Index Server modulhoz a magyar keresőt, amely intelligens nyelvi keresésekre is képes (pl.: a „megy"-re keresve a „ment" és „jön" alakokat is megtalálja...)

Biztonság: azzal, hogy üzleti adataink cseréje egyre inkább hálózatokon keresztül történik, valamint az Internet az üzleti élet szerves részévé lesz, a rendszereink biztonsága is egyre fontosabbá válik.

Webes vásárlás esetén nagyon fontos, hogy a vevő – vagy éppenséggel a bolt – hitelesítése kellően biztonságos legyen. Ha ez nem történik meg, akkor igen könnyen azon kaphatjuk magunkat, hogy mások vásárolnak helyettünk, vagy trójai faló áruházban válogatunk.

A fizetés során átküldött adatokat (mit, és mennyiért vásároltunk, a hitelkártyánk száma, szállítási cím stb.) kellő mértékben el kell rejtenünk ahhoz, hogy mások ne élhessenek vissza a feltört adatokkal. Az átvitt adatok integritásának védelme szintén nehézséget jelent: meg kell akadályoznunk,

Windows 2000 Professional
– az üzleti célú asztali és laptop operációs rendszer

A Windows 2000 Professional a Windows NT Workstation 4.0 utódjaként az üzleti, vállalati felhasználók operációs rendszere. Bár tartalmazza a Windows 98 Second Edition majdnem minden funkcióját, mégsem célja az otthoni és szórakoztató célú alkalmazások futtatása – ez az úgynevezett „consumer" avagy „gaming" platform továbbra is a Windows 98 és utódja, a Windows Millennium marad.

Az alábbi két terület az, ahol a Windows 2000 Professional a legjobb választás a Microsoft operációs rendszerei közül.

Vállalati munkaállomások:

- A továbbfejlesztett, ésszerűsített kezelőfelület számos olyan kényelmi funciót tartalmaz, ami a vállalati felhasználók napi, gyakori munkavégzését egyszerűsíti – például az új My Computer és My Network Places mappák, a testreszabható menük és eszköztárak, az Explorer fejlesztései, a beépített keresés és az automatikus névkiegészítés.
- A munkaállomások karbantarthatóságát segíti a System Recovery Console és a Windows Installer szolgáltatás, mely a teljes alkalmazás-életciklust felügyeli, a telepítéstől a karbantartáson át az eltávolításig.
- A Sysprep, a Remote Installation Preparation (RIPrep) és a Setup Manager lehetővé teszik a munkaállomások nagy mennyiségű, testreszabott automatikus telepítését.
- A Windows File Protection, az újraindítások csökkentett száma, a továbbfejlesztett eszközmeghajtók és a „memórialyukak" kiküszöbölése ipari szintű megbízhatóságot biztosít.
- Január óta Magyarországon is elérhető a Windows 2000 128 bites titkosítást használó változata. Ez és a nyilvános kulcsú titkosítás (PKI, Public Key Infrastucture), a Kerberos alapú felhasználó-azonosítás, valamint az intelligens kártyák (Smart Card) támogatása magas szintű biztonságot garantál.

Laptop számítógépek:

- A hardvereszközök összes képessége kihasználható az ACPI és plug and play támogatásnak köszönhetően.
- Titkosított filerendszer (EFS) az üzletileg érzékeny adatok védelmére, ha elveszítenénk mobil gépünket.
- A hálózaton tárolt adataink minden típusa egyformán kezelhető offline és online állapotban a Synchronization Manager és az ügyféloldali gyorsítótár (Client Side Caching) segítségével – megszabadulhatunk a nagy telefonszámláktól és a 28,8-on csordogáló adatok rémálmától.
- Network Connection Wizard az egyszerűbb Internet-csatlakozáshoz.

hogy közbülső személyek módosíthassák az adatokat, mielőtt még a bolt feldolgozná azokat.

A cégünk partnereivel történő kapcsolattartás újabb gondot vet fel. Nem mondhatjuk meg nekik, hogy milyen operációs rendszert használjanak, mégis kellő biztonsággal kell őket hitelesítenünk.

A felhasználók hitelesítésére: a Unix-világban már régóta használt és bevált, az MIT egyetemen kifejlesztett Kerberos elosztott rendszer szolgál. A Kerberos mellett természetesen a korábbi Windows-hitelesítések, például az NTLM továbbra is használhatók, de ezeket akár le is tilthatjuk. A Kerberos időalapú ticketeket oszt ki a felhasználóknak, akik ezek birtokában érhetik el a szolgáltatásokat. A Kerberos segítségével a tartományok közötti tranzitív megbízotti (trust) kapcsolatok lehetségessé válnak. Ez az „egyszerű" előrelépés erőteljesen megkönnyíti az Active Directory felügyeletét és skálázhatóságát, hiszen nem kell minden menedzselni kívánt tartománnyal szükségszerűen kapcsolatot létrehozni. A hitelesítésről szólva a távoli kapcsolatok során használt PAP, és az abból származtatott CHAP, valamint a MS-CHAP protokollok szabványos továbbfejlesztése, az Extensible Authentication Protocol nagy előrelépést jelent. Ennek segítségével igény esetén új módszerekkel, algoritmusokkal bővíthetjük ki a felhasználói hitelesítés folyamatát. Példaként említhetjük azt, hogy a távoli hálózatokba, a RAS-kiszolgálókba most már intelligens kártyákkal (Smart Card) is beléphetünk. Ezek használata egyébként széles körben támogatott az operációs rendszer használata során, kezelésük integrált szolgáltatás, nincs szükség utólag hozzáadott külső szoftverre. (A Smart Cardok használatát a *Hitelesség 2000 után Smart Card alkalmazásával* című cikkünk ecseteli.)

Aláírt dokumentumok: a dokumentumok hitelességét digitális aláírásunkkal igazolhatjuk, ez a Nyilvános Kulcsú Infrastruktúra (PKI) segítségével történik. A Windows 2000 PKI alapja a kiadványunkban is ismertetett Microsoft Certificate Server (bizonyítványokat kiállító hatóság, CA), amely minden kiszolgálón megtalálható. Feladatai között a felhasználók által használt bizonyítványok kiállítása, ellenőrzése, menedzsmentje és szükség esetén tárolása szerepel. Érdekessége, hogy a Microsoft Certificate Server teljesen integrált az Active Directoryval. Ez azt jelenti, hogy a bizonyítványokat maga a címtár tárolja, tehát ő a felelős azok más telephelyekre történő eljuttatásáért, a bizonyítványokkal kapcsolatos házirendek betartatásáért stb. Ezen kívül – mivel az AD több mesterpéldányos replikációt használ – jóval nagyobb rendelkezésre állást is enged a hagyományos hatóságokkal szemben.

A digitálisan aláírt dokumentumok esetén a túloldali fél nemcsak azt tudja hitelt érdemlően megállapítani, hogy tényleg mi írtuk-e a dokumentumot, hanem az is nyilvánvaló lesz számára, hogy a dokumentumot az adatátvitel közben módosították-e, tehát a webalapú vásárlás egyik újabb kérdése is megoldottnak tekinthető.

Adatok titkosítása: ez a kérdés a publikus hálózatok (pl.: Internet) elterjedésével még időszerűbbé vált, mint valaha. A VPN-ek segítségével távoli, internetes munkaállomásunk mellett is úgy érezhetjük magunkat, mintha közvetlenül a cégünk hálózatára csatlakoztunk volna. Elérhetjük a file-kiszolgálókat, láthatjuk a csak az intraneten hozzáférhető webkiszolgálókat stb. Az Interneten átmenő forgalmat természetesen ezek a megoldások különböző módszerekkel titkosítják.

A Windows 2000 három különböző VPN-megoldást is kínál. A Point-to-Point Tunnelling Protocol segítségével pillanatok alatt működésre bírhatunk bármely VPN-t. A Ciscóval közösen kifejlesztett L2TP hasonlóan egyszerű. Legfőbb előnye, hogy a Cisco eszközök beépítve támogatják.

Az IETF szabványnyá érett IPSec főleg kiszolgálók közötti titkosított adatátvitel során javasolt. Konfigurációja jóval nehézkesebb, mint az előbbi megoldásoké. Az IPSec és az L2TP kombinált használata javasolt azoknak, akik a maximális biztonság mellett a legnagyobb funkcionalitásra törekszenek.

Erős titkosítás: a biztonsággal kapcsolatban most már csak egyetlen nyitott kérdés maradt – mennyire könnyen lehet a titkosítás során használt kulcsokat feltörni? Szakértők szerint a mai gépekkel, gépparkokkal a 128 bites szimmetrikus, valamint az 1024 bites aszimmetrikus (nyilvános, privát) kulcspárokkal titkosított adatokat kellő biztonságban tudhatjuk feltéve, ha magát a privát kulcsunkat biztonságos helyen tároljuk.

A Windows 2000 Server és a Windows 2000 Professional együttes használata

A Windows 2000 Professional vagy a Windows 2000 Server használata már önmagában elérhetővé teszi a Windows 2000-es technológiákat. Mind a munkaállomás, mind a kiszolgálócsalád teljesen kompatibilis és képes együttműködni a korábbi Windows-rendszerekkel. A Professional és a Server együttes használatával azonban teljesen kiaknázhatók a Windows 2000-platform új rendszermenedzsment szolgáltatásai, melyek csökkentik a felügyeleti és az üzemben tartási költségeket. Ilyen menedzsment-szolgáltatások például az alábbiak:

Windows Management Services (rendszer-felügyeleti szolgáltatások):
- Házirend-szolgáltatások (Active Directory);
- Egységesített hardverhozzáférés (WMI);
- Továbbfejlesztett parancsfile-támogatás (WSH);
- Közös rendszer-felügyeleti felhasználói felület (MMC).

Változások és konfigurációk felügyelete:
- Különálló számítógépek felügyelete;
- IntelliMirror: a felhasználói adatok, beállítások és alkalmazások, valamint a távoli operációs rendszertelepítés központosított felügyelete.

A privát kulcs biztonságos tárolására találták ki a korábban már említett és a Windows 2000 által éppen ezért széles körben támogatott Smart Cardokat. A Smart Card önálló kis számítógép memóriával, processzorral.

Lényege, hogy létrehozza a kulcspárunkat, és mivel saját maga képes kriptográfiai műveletek végrehajtására, a kulcsnak soha nem kell elhagynia a kártyát (nem is tudja). Ebből következően a kulcsokat tároló kártyák lemásolása csaknem lehetetlen, legalábbis nagyságrendekkel nagyobb költségeket emésztene fel, mint amennyibe a gépünk merevlemezén tárolt kulcs feltörése kerülne.

A titkosítás során használt kulcsok hosszában jelentős változás következett be 2000. január 14-én. Addig ugyanis az amerikai kormány az Egyesült Államok területén kifejlesztett, külföldre exportálandó szoftverekben használt kulcsok hosszát 56 bitben (szimmetrikus), illetve 512 bitben (nyilvános–privát) korlátozta.

A fenti nappal a kiviteli korlátozás megszűnt, így a Windows 2000 lehetett az első kereskedelmi operációs rendszer, amely az ingyenes „strong crypto patch" feltelepítése után erős titkosítást képes használni az operációs rendszer bármely titkosítási funkciójára. Hazánkban a Windows 2000 Server minden változata ezzel a 128 bites titkosítást használó kiegészítéssel kerül forgalomba.

Alkalmazásplatform

A megbízhatóság növelése, a hatékonyabb rendszermenedzsment, a gazdag infrastrukturális szolgáltatások elsősorban arra szolgálnak, hogy a Windows 2000 platformon futó alkalmazások valóban értéket adjanak a vállalat üzleti tevékenységének. A következőkben áttekintjük, hogy a Windows 2000 hogyan támogatja az alkalmazások fejlesztését, futtatását és karbantartását.

A skálázhatóság tárgyalása során már láttuk, hogy a rendelkezésre állás növeléséhez az alkalmazásokat célszerű több rétegre bontani.

A Windows 2000-et, ahogy a Windows NT korábbi verzióit is, kifejezetten az elosztott, úgynevezett n-rétegű alkalmazások futtatására optimalizálták. A Windows 2000 fejlesztési modellje a Windows DNA, az elosztott hálózati architektúra (Distributed Network Architecture), mely három réteg megvalósításával javasolja az alkalmazások fejlesztését: az adatkezelés, az üzleti logika és a megjelenítés rétegeivel. Nézzük ezeket sorra!

Adatkezelés: a vállalatok informatikai rendszereiben a legfontosabb értéket az évek során felhalmozott adatok jelentik. Bármilyen üzleti alkalmazást vezetünk be, annak a meglévő adatállományt is használnia kell – a konverzió kockázatos és költséges, ezért lehetőség szerint elkerülendő. A Windows 2000 a különböző adatszerkezetek használatához egységes adatelérési technológiákat, nevezetesen az OLE DB-t, az ADO-t, valamint az XML-t kínálja, amelyekkel az alkalmazások a Microsoft és más gyártók relációs adatbázisai mellett a nem strukturált adatokhoz, például a címtárhoz, a file-rendszerhez vagy a levelező és csoportmunka-támogató rendszerekhez is hozzáférhetnek.

Sok magyar cégnél az is gondot jelent, hogy nem lehet lecserélni a meglévő adatbázisokat az áttérés költségei miatt – a régi adatbázis-kezelő rendszer pedig behatárolja az alkalmazásfejlesztési lehetőségeket is. Az egységes adatelérés azzal oldja fel ezt a konfliktust, hogy az adatbázis formátumától függetlenül szabadon választhatunk a fejlesztőkörnyezetet.

Üzleti logika: a vállalatok üzleti folyamatainak összessége szintén kiemelt értéket képvisel a cégek életében. A vállalati rendszerek célja éppen ezeknek a folyamatoknak a felgyorsítása és hatékonyabbá tétele az informatikai eszközökkel történő leképezés segítségével. Ez az úgynevezett üzleti logika rétegben történik, amelyet pedig a leghatékonyabban az összetevők testesítik meg, a Windows DNA esetében egészen pontosan a COM+ összetevők. A Windows 2000 gazdag környezetet teremt az összetevők futtatásához: automatikusan kezeli az általuk használt erőforrásokat, felügyeli a végrehajtott tranzakciókat, létrehozza a kommunikációs hátteret, valamint a védelmet és a menedzselhetőséget.

A skálázhatóság tárgyalása során már láttuk, hogy az alkalmazások középső rétegének komponensekre bontása a COM+ terheléselosztás (CLBS) szempontjából igen előnyös. A teljesítmény növelésekor azonban sokkal lényegesebb az, hogy komponenstechnológia használata esetén az egyes üzleti részfolyamatok módosításakor, illetve megváltozása során a kiszolgálóra telepített összetevők szükség esetén könnyen lecserélhetők a többi komponens módosítása nélkül.

A fentiek előnye leginkább az n-rétegű rendszerfelépítést megelőző fejlesztési modell, az úgynevezett ügyfél-kiszolgáló architektúra példáján szemléltethető legjobban. Az ügyfél–kiszolgáló elvű alkalmazások esetében az üzleti logika nagy része az ügyfélgépeken futó „kövér", vagy „vastag" alkalmazásokban található. Ez egyben azt is jelenti, hogy a vállalati folyamatok minden egyes megváltozása során az összes ügyfélgépet frissítenünk kell. A többrétegű modellben az üzleti logikát megtestesítő összetevők egy vagy több dedikált alkalmazás-kiszolgálón találhatók, változás esetén csak ezeket kell módosítani. Az ügyfélgépeken található front-end alkalmazás csak az adatok megjelenítését végzi.

Megjelenítés: az előbbi gondolatmenetből az is látható, hogy a Windows 2000 által támogatott többrétegű alkalmazásmodell csökkenti az ügyfélgépek üzemeltetési költségeit is. Sokan úgy gondolják, hogy ez a költségcsökkenés csak a Windows 2000 Professional ügyféloldali használatakor jelentkezik – a vállalatok többségében a géppark azonban nem áll olyan szinten, hogy a Windows 2000 Professional bevezetését hardverbővítés nélkül el tudnák végezni.

Habár a Windows 2000 Professional egyértelműen az üzleti környezet optimális ügyféloldali operációs rendszere, ez még-

sem jelenti azt, hogy a hardverkövetelményeket nem teljesítő gépeket ki kell dobni. A Terminal Services a Windows 2000 Server család integrált része (azaz a Windows NT 4.0-val ellentétben nem külön termék), amellyel a legkorszerűbb 32 bites alkalmazások gyengébb ügyfélgépeken, vagy éppen úgynevezett Windows-alapú terminálokon is futtathatók.

Az Internet szintén fontos alkalmazási környezet: ha valamelyik vállalat a saját szolgáltatásait és adatait elérhetővé teszi a világhálón keresztül, akkor nem követelheti meg az ügyféloldalon sem az operációs rendszert, sem az alkalmazást – ezzel szemben a legkülönfélébb képességű böngészők támogatására kell felkészülnie. A Windows 2000 részét képező Internet Information Services mind a „legnagyobb közös osztónak" számító HTML 3.2-t, mind pedig a legfejlettebb, már-már natív felületű kiegészítőket támogatja.

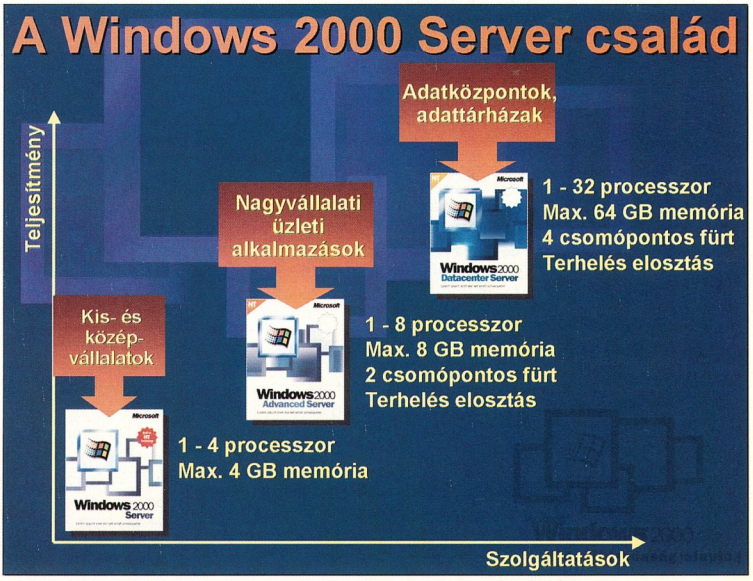
COM+: a Windows DNA rétegei közül a vállalati működés szempontjából egyértelműen a középső réteg, az üzleti logika a legfontosabb – az ebben található Windows 2000 komponensszolgáltatások a Microsoft komponensmodelljére, a COM-ra épülnek, melynek Windows 2000-es verzióját nevezzük COM+-nak. Ennek a modellnek a lényege nem is annyira az alkalmazások futtatásához nyújtott „fizikai" segítség, hanem az, hogy megkíméli a programozót a rutinfeladatok ismételt elvégzésétől. Ha valaki adott, a COM+ környezetbe szánt alkalmazás összetevőit fejleszti, nem kell azzal törődnie, hogy azok, tíz vagy ezer felhasználót szolgálnak-e ki, hogy közel lesznek-e az adatforrásokhoz vagy távol, hogy használnak-e tranzakciókat vagy sem, hogy szolgáltatásaikat védeni kell-e vagy sem; ezeket ráér később, a rendszer üzembe állításakor beállítani, és nem neki kell leprogramozni. Más szóval a fejlesztő a tényleges üzleti feladat megoldására koncentrálhat a házimunkák és rutinkódolás (népszerűbb néven „favágás") elvégzése helyett.

A COM+ szolgáltatásai közül kiemelendő az Internet Information Services, amely a jól ismert IIS 5.0-s változata, azonban mostantól már nem önálló termék, hanem az operációs rendszer beépített szolgáltatása, erre utal a névváltoztatás is (Serverről Service-re). Az IIS a webes alkalmazások nagy teljesítményű futtatókörnyezete, mely nagy méretű kereskedelmi célú webhelyek alapja lehet (illetve már az is, hiszen többek között például a Barnes and Noble webes könyvkereskedés, a Dell.com, a Nasdaq elektronikus tőzsde már Windows 2000-en fut.)

A másik fontos szolgáltatás a Message Queuing Services, amely elsősorban az elosztott rendszerek esetében hasznos. Ha valamelyik vállalati alkalmazás több gépen fut, melyek különböző telephelyeken találhatók, és ezeket a telephelyeket kevésbé megbízható, vagy szakaszos rendelkezésre állású vonalak kötik össze, a Message Queueing Services aszinkron üzenettovábbító szolgáltatása ki tudja küszöbölni a telekommunikációs nehézségeket. A fejlesztőnek így nem kell törődnie azzal, hogy az alkalmazás online vagy offline állapotban fut-e, ezt az MSMQ automatikusan kezeli, így a hálózati hibák kezelését sem kell külön kódolni.

Rendszerszolgáltatások és fejlesztőeszközök: a fent említett három réteg mellett az alkalmazások fejlesztéséhez szükség van még rendszerszolgáltatásokra, például a felhasználók, számítógépek, alkalmazások adatait tároló címtárra, a védelmi eszközökre és a rendszer-felügyeleti infrastruktúrára.

A Windows 2000-ban ezek az Active Directory, az Intelli-Mirror és más, korábban bemutatott technológiák segítségével valósulnak meg. Ne feledkezzünk meg a fejlesztőkörnyezetekről sem: a Windows 2000-platform nagyon népszerű, a Microsoft Visual Studio mellett más szoftvergyártók fejlesztőeszkö-



zei is erőteljesen támogatják. Ami talán a Microsoft megoldását a többi fölé emeli, az a Microsoft Solutions Framework (MSF), mely fejlesztési módszertant ad az n-rétegű, elosztott alkalmazások készítéséhez.

Összefoglalás

A Windows 2000-platform technológiailag nagyon szerteágazó, bonyolult, néha talán sokkoló is (a részletes technikai dokumentációt tartalmazó Windows 2000 Resource Kit hat vaskos kötetben fog megjelenni). Éppen ezért a szakmának alaposan fel kell készülnie rá mind a rendszerintegrátorok és fejlesztők, mind a felhasználók és üzemeltetők oldalán. A fenti áttekintés talán segített abban, hogy az egyes szolgáltatások és technológiák összekapcsolódásait és a vállalati rendszerbe való integrálási irányait bemutassa.

Az áttekintés után a CHIPtár további cikkei az egyes területeket részletesebben, mélységeiben mutatják be, melyeket a Microsoft Magyarország terméktámogatási- és rendszermérnökei, konzulensei, illetve a magyarországi Microsoft partnercégek mérnökei írtak. Nekik ezúton is szeretném megköszönni a kiváló munkát.

Windows 2000 Server

A Windows 2000 Server általános, többcélú hálózati kiszolgáló operációs rendszer, amely tetszőleges vállalati méret esetén képes az alapvető hálózati- és alkalmazás-kiszolgáló funkciók megteremtésére. Az alábbiak bemutatják, hogy a Windows 2000 Server milyen technológiai újdonságokat hoz a jellemzően vállalati kiszolgáló szerepkörökben.

File-kiszolgálók:

- Az Active Directory címtárszolgáltatás segítségével a megosztott könyvtárak és file-ok könnyebben megtalálhatók.
- Az indexelt file-rendszer a dokumentumok tartalmát is képes indexelni, így a felhasználók akár a tartalmuk alapján könnyen fellelhetünk egy adott dokumentumot.
- Az elosztott file-rendszer (Distributed File System – DFS) segítségével a vállalatok több file-rendszert átölelő, nagy megbízhatóságú file-kiszolgálókat telepíthetnek.
- A dinamikus kötetfelügyelet (Dynamic Volume Management) leállás nélkül képes kezelni a kiszolgáló háttértárait.
- A hierarchikus tároló-felügyelet (Hierarchical Storage Management – HSM) a ritkábban használt adatokat automatikusan olcsóbb médiára (például szalagra) menti.
- A többféle protokoll segítségével a Windows ügyfelekhez hasonlóan Novell, Unix és Macintosh ügyfelek számára is nyújthatunk file-szolgáltatást.
- A lemezkvótákkal az igénybe vehető háttértár-terület mérete felhasználónként szabályozható.
- A kiszolgálón található file-ok titkosíthatók, sőt ezek a szalagos adatmentésben is automatikusan titkosítva jelennek meg.

Nyomtató-kiszolgálók:

- A nyomtatók az Active Directory szolgáltatás segítségével a helyszín és a tulajdonságaik alapján is kereshetők.
- A Windows 2000 nyomtató, illetve nyomtatási protokoll támogatása jelentősen bővült.
- A továbbfejlesztett felhasználói felügyelet csökkenti az üzemeltetési költségeket.
- Az Internet Printing Protocol támogatásával az Interneten keresztül is nyomtathatunk megosztott nyomtatókra.

Webkiszolgálók:

- A kiszolgált webhelyek között a processzor felhasználásának korlátozásával a CPU-idő felosztható (CPU-throttling).
- A felhasználók a WebDAV (Distributed Authoring and Versioning) támogatásával könnyen publikálhatják, kezelhetik és megoszthatják adataikat a weben.
- Az új varázslók segítségével a rendszergazda könnyen felügyelheti a webkiszolgáló biztonsági, valamint azonosítási és SSL beállításait.

Alkalmazás-kiszolgálók:

- A beépített, széleskörű alkalmazás-szolgáltatások – összetevők, parancsfile-ok, tranzakciós és sorkezelő szolgáltatások segítségével méretezhetőbb, megbízhatóbb alkalmazások készíthetők rövidebb idő alatt.
- A továbbfejlesztett Internet-szolgáltatásoknak köszönhetően a webes felülettel ellátott alkalmazások fejlesztése még könnyebb.

Hálózati és kommunikációs kiszolgálók:

- Az új titkosítási és azonosítási eljárások segítségével a biztonságos hálózati forgalom többféle módon is megteremthető.
- A felhasználók könnyebben hozhatnak létre internetes kapcsolatokat az új kapcsolatkezelő segítségével.
- Megvalósították a TCP/IP protokoll legújabb szabványait a nagy sávszélességű hálózatok teljesítményének kihasználása céljából.
- A dinamikus DNS könnyebb hálózati felügyeletet nyújt.
- A Windows Quality of Service és a Multicast forwarding segítségével felügyelhetjük a hálózati sávszélességet, és elősegíthetjük az adatok közvetlen és gyors továbbítását.
- A multimédiát támogató protokollok segítségével hang-, videó- és adathálózatokat építhetünk ki.

Vállalati alapkiszolgálók (Infrastruktúra-kiszolgálók):
- Az üzleti alkalmazások globálisan felügyelhetők és kezelhetők az Active Directory szolgáltatás segítségével.
- Az elosztott biztonsági szolgáltatások egyaránt nagyobb biztonságot nyújtanak a vállalati, az Internet és az extranet környezetben.
- A vállalati szinten alkalmazott hitelesítéseket a teljes körű, nyílt kulcsú infrastruktúra-szolgáltatás kezeli és hozza létre.
- A Windows Management Services a központosított rendszerfelügyelet, a továbbfejlesztett hardverfelügyelet és az egyedi parancsfile-ok használatának alapja.
- Az IntelliMirror rendszer-felügyeleti megoldásainak köszönhetően a felhasználók adatai, alkalmazásai, saját beállításai és az általuk használt operációs rendszerek központosítva, egyszerűen felügyelhetők.

Windows 2000 Advanced Server

A Windows 2000 Advanced Server a Windows 2000 Server minden, az előbbiekben felsorolt szolgáltatása mellett az alábbi – nagyobb, robosztusabb kiszolgálók létrehozását megkönnyítő – jellemzőkkel bír:

Jobb méretezhetőség:
- A Windows 2000 Advanced Server akár 8 processzoros SMP-kiszolgálóként is működhet.
- A nagy méretű memória támogatásával az Intel (PAE-alapú) rendszereken a maximálisan kihasználható memória mérete 8 GB-ra nőtt.
- Legfeljebb 32 pontos hálózati terheléselosztás (Network Load Balancing).

Nagyobb rendelkezésre állás:
- A Server Clustering Services nagy rendelkezésre állású – kétpontos – fürtök létrehozását teszi lehetővé hagyományos PC-s hardveren.

Jobb kezelhetőség:
- Kiszolgálófürtök és folyamatos rendszerfrissítés.
- A Cluster Automation Server segíti a fürtözést kihasználó alkalmazások fejlesztését.
- Adatmentő és replikációs API-k a fürterőforrások mentésére.
- A Job Object API támogatásával a processzek csoportját egy egységként kezelhetjük és felügyelhetjük.

Windows 2000 Datacenter Server

A Windows 2000 Datacenter Server a Windows 2000 Advanced Server változat minden szolgáltatása mellett az alábbi – igazán nagy rendszerek kiépítésére alkalmazható – szolgáltatásokat tartalmazza:

Jobb méretezhetőség:
- 32 utas SMP kiszolgáló (Windows 2000 Datacenter Server akár 32 processzoros rendszerben).
- Nagy méretű memória támogatása – Intel (PAE) rendszerben akár 64 GB.
- A Winsock Direct meggyorsítja a processzek hálózaton keresztüli kommunikációját.

Nagyobb rendelkezésre állás:
- A Server Clustering Services segítségével akár négypontos fürtöket is kiépíthetünk.

Jobb kezelhetőség:
- A Process Control Manager segítségével felügyelhetjük a kritikus kiszolgáló-erőforrásokat.

Jellemző	Windows 2000 Professional	Windows 2000 Server	Windows 2000 Advanced Server	Windows 2000 Datacenter Server
Processzorok száma	2	4	8	32
Felhasználható memória	4 GB Intel	4 GB Intel	8 GB Intel (PAE)	64 GB Intel (PAE)
Hálózati terhelés-elosztás (NLB)	Nincs	Nincs	Van (max. 32 csomópont)	Van (max. 32 csomópont)
Kiszolgálók fürtözése	Nincs	Nincs	Van (max. 2 csomópont)	Van (max. 4 csomópont)
Job Object	Job Object API	Job Object API	Job Object API	Process Control Manager
WinSock Direct	Nincs	Nincs	Nincs	Van
Hardver-kompatibilitási lista (HCL)	Van	Van	Van	Gold HCL

A felhasználói termelékenység növelése

Tény, hogy az egyszerűen használható operációs rendszereket olcsóbb üzemeltetni, és az is, hogy a Windows 2000 újításainak köszönhetően az eddigi legkönnyebben használható Windows. De mitől is lesz az új rendszer felhasználója termelékenyebb?

Az elmúlt évtized során az asztali és notebook számítógépek, valamint az operációs rendszerek technológiájának jelentős fejlődése és az árak számottevő csökkenése teljesen átalakította az üzleti világot. A technológiai fejlesztések és a továbbfejlesztett hálózati lehetőségek összekapcsolják a vállalat osztályait, az adatokat, valamint elősegítik a fizikai, illetve szervezeti határokon átívelő kommunikációt. Napjainkban az irodai alkalmazottak munkájuknak legalább egy részét vagy annak egészét számítógépeken végzik.

Ahogy a személyi számítógépek és az operációs rendszerek egyre nagyobb tudásúvá válnak, használatuk is egyre bonyolultabb lesz. Míg néhány felhasználó ki tudja használni az új funkciók előnyeit, sokan egyáltalán nem, emiatt a vállalat számítógépes beruházásainak megtérülése is csökkenhet. Ha a felhasználók nem használják ki teljesen az új számítógépek lehetőségeit, a vállalat nem tudja igazolni a számítógép költségét az általa bekövetkezett termelékenység-növekedéssel, ráadásul bizonyos esetekben a bonyolultabb rendszer a vállalat karbantartási és oktatási költségeit is növelheti.

Az alábbiakban megpróbáljuk részletesen bemutatni, hogy a Windows 2000 továbbfejlesztései hogyan teszik e rendszert egyszerűbben használhatóvá, és mivel segítik a felhasználókat abban, hogy a lehető legnagyobb mértékben kihasználhassák az új lehetőségeket.

Az egyszerűbben használható Windows létrehozása

Mivel az operációs rendszer jóformán az egyetlen szoftver, amelyet mindenkinek használnia kell, gyakran kulcsszerepet játszik a számítógép bonyolultságának és költségességének meghatározásában.

A Windows 2000 tervezése során a Microsoft először megvizsgálta, hogy a különféle típusú felhasználók hogyan kezelik az operációs rendszereket, azzal a szándékkal, hogy megtudja, hogyan alkalmazzák az üzleti életben a számítógép funkcióinak és teljesítményének előnyeit.

A vásárlói visszajelzések gondos elemzése után sokat változtattak az operációs rendszeren azért, hogy növeljék a felhasználók termelékenységét és csökkentsék a tulajdonlás költségét (a TCO-t).

Az alábbiakban a következő továbbfejlesztett lehetőségeket mutatjuk be:

- **Egyszerűbb telepítés:**
  Az egyszerűsített, megbízhatóbb telepítőprogram a telepítési parancsfile-okat is támogatja, így minimális felhasználói közreműködés szükséges az installáláshoz.
- **Jobban testre szabható és hatékonyabban használható Windows Asztal:**
  Egyrészt még jobban testre szabhatjuk az *Asztalt*, másrészt a rendszer automatikusan alkalmazkodik rendszerkezelési szokásainkhoz.
- **A dokumentumok és erőforrások könnyebb elérése:**
  A felhasználó minden file-ja központi helyre (a *My Documents* mappába) kerül, így egyszerűbb megtalálni és lementeni őket. Emellett a kereső funkció is fejlődött, valamint kibővült a hálózati keresés lehetőségével. Ezáltal olyan dokumentumok és erőforrások is könnyedén fellelhetők, amelyek nem a saját számítógépünkön találhatók.

- **Nagyobb megbízhatóság és a beállítások módosításának támogatása:**
  A Windows 2000 támogatja az önjavító alkalmazásokat, a plug and playt és az energiagazdálkodást, ezáltal a rendszer stabilitásának veszélyeztetése és jelentős leállási idő nélkül lehet hardverelemeket és alkalmazásokat telepíteni.

Vágjunk bele!

Az első fejlesztések már a telepítés során felbukkannak: az installáció lényegesen egyszerűbb mind a telepítő parancsfile-okkal, mind ezek nélkül, valamint játszi könnyedséggel építhetünk kis hálózatokat.

A telepítés

A telepítés az új operációs rendszer használatának legbonyolultabb része lehet. Ahol van rendszergazda, ott a felhasználóknak egyszerűbb a dolga, ugyanis az adminisztrátor által létrehozott telepítési parancsfile-ok megválaszolják helyettük a telepítéskor és a rendszer első futtatása során felbukkanó kérdések legtöbbjét. Az erre szolgáló eszközök technikai korlátai azonban igen nehézzé teszik az olyan parancsfile-ok létrehozását, amelyek minden kérdésre válaszolnak. Emellett, ha a telepítés során előre kiszámíthatatlan, vagy a parancsfile által nem kezelt esemény történik, a telepítés gyakran leáll, és a felhasználó így kénytelen a rendszergazdához fordulni. Sok vállalat használ elektronikus szoftverelosztó eszközöket, például Microsoft System Management Servert, és bár ezek a termékek egyszerűbbé teszik a telepítést a felhasználók számára, bizonyos technikai korlátok miatt mégsem használhatók minden esetben.

A Windows 2000 egyik legfontosabb fejlesztési célja az volt, hogy a telepítés jelentősen egyszerűbbé váljon a felhasználók számára. Nem parancsfile-ra épülő telepítés esetén a következő előnyöket élvezhetjük:

- **Egyszerűbb telepítés:** a telepítés során megjelenő ablakok és kérdések nem szaknyelven, hanem könnyen érthető formában íródtak. Az egyik telepítési ablak például egyszerűen azt kérdezi, hogy ki használja majd a számítógépet („Who is using this computer?"). A választól függően az operációs rendszer automatikusan beállítja a felhasználónak megfelelő biztonsági szintet.
- **Automatizált feladatok:** míg a Windows NT korábbi verzióinak telepítőprogramjai feltételezték, hogy a felhasználók ismerik a számítógépet, és képesek minden kérdésre válaszolni, a Windows 2000 kevesebbet kérdez, és többet feltételez.
  A telepítést végző személy például automatikusan felhasználóvá is válik, míg korábban ehhez a telepítés befejezése után külön eszközt kellett igénybe vennie. A Windows 2000 támogatja a plug and playt is, azaz automatikusan beállítja a hardvereszközöket, és telepíti meghajtóprogramjaikat is.
- **Megbízhatóbb telepítés:** a korábbi Telepítők azonnal leálltak, ha valamilyen hiba lépett fel, még akkor is, ha az nem volt kritikus. Ezzel szemben, ha a Windows 2000 telepítése során nem kritikus gond lép fel – vagyis olyan, amitől a számítógép még el tud indulni –, a telepítés folytatódik, majd a procedúra befejeztével jelentést kapunk a rendszergazdára váró megoldandó problémák listájával.

A telepítési folyamat fejlesztései olyan környezetekben a leglátványosabbak, amelyekben a rendszergazdák telepítési parancsfile-okat használnak az elektronikus szoftverelosztási eszközökhöz. A grafikus felületű Setup Manager használatával a rendszergazda a telepítés majdnem minden részletét automatizálhatja – például elérheti, hogy a felhasználói név és jelszó bekérése után a rendszer automatikusan a megfelelő módon állítsa be önmagát. A programmal olyan gyakori feladatokat is automatizálhatunk, mint például adott rendszer konfigurálása a vállalati hálózat igényeinek megfelelően. A Setup Manager fejlesztői a jövőre is gondoltak, így a telepítés során újabb, a Windows 2000 alapcsomagból hiányzó komponenseket és eszközmeghajtókat is fel tud rakni.

A bejelentkezés

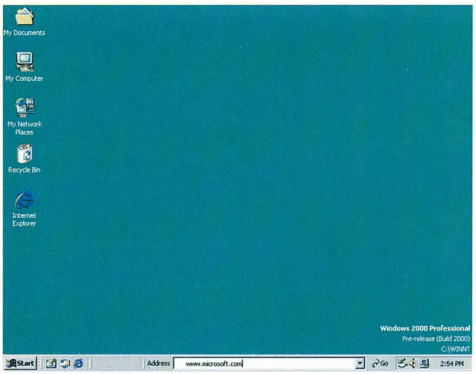
Az új bejelentkező ablak alapértelmezésben nem jeleníti meg a tartományneveket, mivel a felhasználók csak igen ritkán váltanak tartományt, viszont gyakran előfordult, hogy véletlenül elállították. A karbantartási költségek szempontjából tehát ez a kedvezőbb megoldás. A rendszer egyéb újdonságokat is tartogat a bejelentkezés terén, ilyen például a kerberosos beléptetés, amely sokkal gyorsabb és biztonságosabb lehet a jelenleg alkalmazott megoldásoknál (lásd még a *Hitelesség 2000 után Smart Card alkalmazásával* című cikkünket).

Kis hálózatok létrehozása

A nyomtatók megosztásához és a file-ok cseréjéhez sok üzleti felhasználó épít apró hálózatokat. Ezt a feladatot a Windows 2000 nagyon leegyszerűsíti – elég mindössze egy hubhoz kapcsolni a Windows 2000-es gépeket, a többi beállításról már a rendszer gondoskodik. Amikor a Windows 2000 Professional először elindul, megpróbál olyan DHCP (Dynamic Host Configuration Protocol) kiszolgálót találni, amely megadja neki azt a címet, amely alapján a hálózat többi gépe megtalálhatja. Ha – a kisvállalkozások esetében jellemző módon – ez nem sikerül, akkor automatikusan olyan módba állítja önmagát, amelyben képes a hubhoz csatlakoztatott többi Windows 2000-alapú gép fellelésére. Amennyiben újabb Windows 2000-es masinákat csatolunk a hubra, ezek is automatikusan bekapcsolódnak a munkacsoportba. Ezt a lehetőséget automatikus IP-címzésnek hívják, és további részletek a Windows 2000 Professional Technical Overview-ban találhatók róla.

A továbbfejlesztett Asztal

Ahogy a számítógépek egyre használhatóbbakká válnak, többnyire bonyolultabbak is lesznek. Az utóbbi néhány évben a Desktop – sok alkalmazott alapvető munkafelülete – egyre



A Windows 2000 Professional Asztala kevésbé zsúfolt és könnyebben testre szabható

zsúfoltabbá vált. Emellett, ahogy a számítógépek egyre több feladat ellátására váltak képessé, a felhasználók egyre nehezebben tudták „felderíteni" az egyes feladatok elvégzéséhez szükséges lépéseket. A legtöbb felhasználó nem olvassa el a használati útmutatót, és nem hajlandó sok időt áldozni új feladatok megtanulására. A Windows 2000 az Asztal környékén sok olyan finomítást tartalmaz, amelyek hatékonyabbá teszik a felhasználó munkáját. Maga az Asztal jobban testre szabható, a környezet pedig automatikusan alkalmazkodik a felhasználó rendszerkezelési szokásaihoz.

A testre szabott menük (Personalized Menus)

Az átlagos felhasználó a számítógép élettartama alatt több tucat alkalmazást telepít. Ez általában sok bejegyzést tartalmazó, zsúfolt Start menüt eredményez, amelyről néhány programot naponta használunk, a legtöbbet viszont csak alkalmanként.

A Windows 2000 folyamatosan figyeli, hogy melyik menüpontot milyen gyakran használjuk, és csak a legnépszerűbbeket jeleníti meg. A többi alkalmazás csak akkor bukkan fel, ha az egérrel ráállunk a menü alján elhelyezkedő kettős nyílra.

E funkció sokkal kevésbé zsúfolt Asztalt eredményez, így a felhasználók gyorsan hozzáférhetnek a leggyakrabban használt programokhoz. A megjelenített menüelemek dinamikusan változnak: ha adott alkalmazást elkezdünk gyakran használni, az egyre feljebb kerül a menüben.

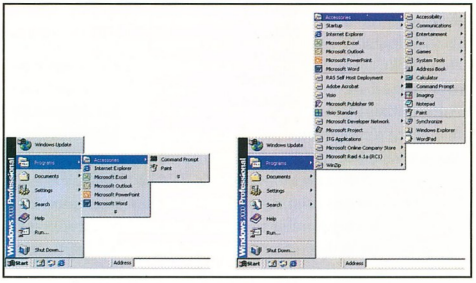
A nemrég használt elemek listája (Most Recently Used List)

A legtöbb felhasználó úgy szabja testre az Asztalt, hogy könnyen hozzáférhessen a leggyakrabban használt erőforrásokhoz, például állandó kapcsolatot létesít olyan megosztott hálózati mappákhoz, amelyekben a munkacsoport a fontos megosztott dokumentumokat (pl.: marketingterveket vagy termékspecifikációkat) tárolja. Amikor azonban ritkán használt erőforrásokat kell megkeresniük, a termelékenységük azonnal lecsökken. Ha például olyan bemutatósablonra van szükségük, amelyet általában a vállalat másik csoportja használ, akkor meg kell keresniük az ezt tartalmazó megosztott hálózati mappát – általában úgy, hogy kapcsolatba lépnek valakivel az illető csoportból. Mikor a mappa végre megvan, valószínűleg nem hoznak létre állandó kapcsolatot hozzá, mivel nem számítanak rá, hogy még egyszer szükségük lesz rá. Ha ezután néhány héttel később mégiscsak szükségük támad valamelyik másik sablonra is, valószínűleg újra végig kell járniuk a fenti lépéseket.

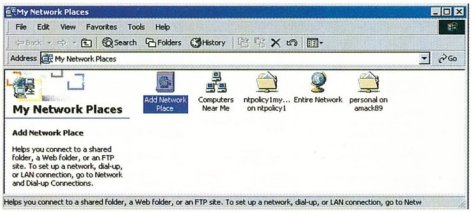
A leggyakrabban használt elemek listája (*Most Frequently Used list*) sokkal egyszerűbbé teszi az ilyen feladatok elvégzését. A rendszer figyelemmel kíséri, hogy a felhasználó milyen erőforrásokat használt, és ezekről a megfelelő helyen listát vezet. A továbbfejlesztett *My Network Places* mappa például az elért hálózati helyekről tart fenn listát, amelybe azok a helyek is bekerülnek, amelyekhez a felhasználó nem hozott létre állandó kapcsolatot. A gyakori elemek listája a Windows 2000 felület sok helyén megjelenik, köztük a *Keresés* (*Search*), és a *Megnyitás/mentés* (*Open/Save*) párbeszédpaneleken is.

Az automatikus kiegészítés (AutoComplete)

A mindennapos feladatok elvégzéséhez (pl.: adott file elmentéséhez vagy valamilyen webcím eléréséhez) a felhasználóknak különböző információkat kell pontosan begépelniük, amit általában könnyű elrontani, és nehéz megjegyezni. Az automatikus kiegészítés (*AutoComplete*) először az Internet Explorer 4-ben bukkant fel; ott a hosszú, összetett URL-ek beírásában segített (például, ha beírjuk, hogy www.micr, az AutoComplete kiegészíti www.microsoft.com-má). Ez a válto-



A testre szabott menükben csak a leggyakrabban használt elemek jelennek meg. A többi menüpont akkor bukkan fel, ha az egérrel a kettős nyílra állunk



A My Network Placesben mindazok a mappák és erőforrások megtalálhatók, amelyeket a felhasználó meglátogatott a hálózaton

zat még csak azokat a helyeket tudta kiegészíteni, ahol korábban már jártunk.

A Windows 2000 jelentősen továbbfejlesztette az AutoComplete funkciót, és használatát az egész felületre kiterjesztette (nem csak az URL-ek beírásakor működik). Az egyik fő fejlesztés, hogy ha az AutoComplete felismer valamilyen szöveget, akkor ahelyett, hogy kiegészítené azt, legördülő ablakban az összes lehetőséget felsorolja. A másik, hogy már keresni is tud, ha például valamelyik felhasználó azt írja be, hogy „\\wpg\u", akkor megjelenik a mappa „u" betűvel kezdődő állományainak listája. A Windows 2000 lépten-nyomon használja az AutoComplete-et: a párbeszédpaneleken, a *Futtatásban* (*Run*), az űrlapokon és a hálózati meghajtók megkeresésében, valamint a *Windows Intézőben* (*Explorer*).

A Start menü beállításai

A Windows 2000 a Start menü testre szabására több lehetőséget nyújt: meghatározhatjuk például, hogy a *Kedvencek* (*Favorites*) és a *Dokumentumok* (*My Documents*) mappa megjelenjen-e. Ezen kívül többek között a *Hálózati kapcsolatok* (*Network Connections*) és a *Nyomtatók* (*Printers*) mappát is beépíthetjük a menübe.

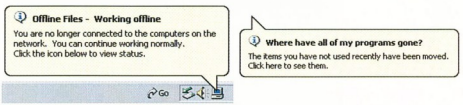
Más fontos fejlesztések

- **A Súgóbuborék (Balloon Help)**

A korábbi aprócska tooltipek helyét bőséges információt nyújtó súgóbuborékok vették át, amelyek változatlanul akkor jelennek meg, ha a kurzort valamelyik ikonra állítjuk. Az így kapott részletesebb leírás segít a felhasználóknak, hogy minél gyorsabban megismerkedjenek az új rendszer továbbfejlesztett szolgáltatásaival. Amikor például a testre szabott menü először jelenik meg, egy buborék elmagyarázza a felhasználónak, hogy mire számítson.

- **Testre szabható eszköztárak**

A *Windows Intéző* (*Explorer*) eszköztár többféleképpen is testre szabható. A vállalatok például egyedi gombokat hozhatnak létre az alkalmazottak egyes feladatainak megkönnyítésére, mondjuk a vállalati intranet site elérésére.



A Súgóbuborék segít felkutatni a Windows 2000 újdonságait

- **Egyszerűsített *Sajátgép* (*My Computer*) mappa**

A My Computer mappát átszervezték, már csak a számítógéphez tartozó tárolóeszközöket és a *Vezérlőpult* ikonját tartalmazza. A *Telefonos hálózat* (*Dial-Up Networking*) és az *Ütemezett feladatok* (*Scheduled tasks*) átkerült a Vezérlőpultra, ugyanis vezérlési feladatokat ellátó eszközökről lévén szó ez megfelelőbb hely számukra.

- **Továbbfejlesztett *My Network Places* mappa**

A *My Network Neighborhood* új nevet kapott, és már a hálózat minden megosztott számítógépét, file-ját, mappáját, nyomtatóját és egyéb erőforrását képes megjeleníteni.

- **Részletesebb *Súgó***

A Windows 2000 továbbfejlesztett súgófunkciójának jellemzői: egységes stílus, szerkezet és terminológia; jól használható *Tartalom karton*; kevesebb szint; nagyobb, részletesebb index; integrált *Hibaelhárítók* (*Troubleshooters*); a gyakori feladatok hangsúlyozása; több parancsikon a *Súgóból* történő összetevő-indításhoz; a *Kapcsolódó témakörök* (*Related Topics*) linkek kiterjedt használata.

- **Rendszerüzenetek**

Ha lehetséges, a Windows 2000 hibaüzenetei nemcsak azt közlik a felhasználóval, hogy hiba történt, hanem azt is, hogy mit tehet annak kijavítása érdekében. Az üzenetek az elhárításhoz szükséges eszközöket és a kapcsolódó *Súgótémaköröket* is felsorolják, így a felhasználható legközelebb már megelőzheti a hibát. A felhasználói közreműködésre felszólító hibaüzenetek (ezek az operációs rendszer stabilitására is hatást gyakorló hibákra figyelmeztetnek) különböznek az egyszerű informáló üzenetektől, ez utóbbiak egy idő után automatikusan el is tűnnek.

Dokumentumok és file-ok kezelése

Mint már korábban írtuk, a Windows 2000 leegyszerűsíti a dokumentumok és file-ok kezelését. A kényelmesebb munkában a file-ok központi tárlóhelyéül szolgáló My Documents mappa, a továbbfejlesztett kereső, az automatikus file-szinkronizálás, valamint az e-mail mellékletként érkezett dokumentumok rugalmasabb kezelése játszik szerepet.

A My Documents mappa

Mivel az alkalmazások nem adott helyre mentik a file-okat, egy-egy elmentett file megtalálása gyakran okoz gondot. Néhány alkalmazás például olyan mappákba ment, amelyeket ma-

ga az alkalmazás hozott létre automatikusan; néhány alkalmazás pedig nem határozza meg, hogy a mentett file-ok hova kerüljenek, így az alapértelmezett system32 könyvtárban dolgoznak. Veszélyes a system32 könyvtárba menteni, mivel a rendszer file-jai is itt találhatók, ezek módosítása pedig megzavarhatja a gép működését.

Ez az összevisszaság megnehezítette mind a felhasználók, mind a rendszergazdák munkáját, mivel nem mindig találták meg az összes olyan dokumentumot, amelyről biztonsági másolatot akartak készíteni. A Windows 2000-ben a My Documents mappa jelentősen továbbfejlődött, és az információk elmentésének és megkeresésének állandó helyévé vált. Ha az alkalmazás nem igényli kifejezetten, hogy másik mappába menthessen, a Windows 2000 átirányítja a *My Documentsbe*. Mivel a csoportos házirendben (Group Policy) a rendszergazda már e mappa elérési útját is beállíthatja, még egyszerűbb rábírni a felhasználókat, hogy biztonságos hálózati helyen tárolják adataikat.

A My Documents tartalma felhasználónként, megfelelő jogosultságokkal védve tárolódik, így még az egyazon gépen dolgozó felhasználók sem pillanthatnak bele egymás dokumentumaiba.

• **A *My Pictures***

A My Documentsben található My Pictures mappa beépített képnézegető funkcióinak köszönhetően egyszerűbbé teszi a képek kezelését.

A My Pictures az összes fontosabb feladatra képes, beleértve a nagyítást és a teljes méretű vagy kicsinyített (thumbnail) megjelenítést, így az esetek többségében megtakaríthatjuk a képszerkesztő alkalmazások elindítását. Érdekes adalék, hogy ha a kép NTFS file-rendszert használó meghajtón található, a jellemzőiről szöveges leírást is készíthetünk a *Tulajdonságok* ablakban (pl.: cím, tárgy és kategória).

Információk és erőforrások keresése

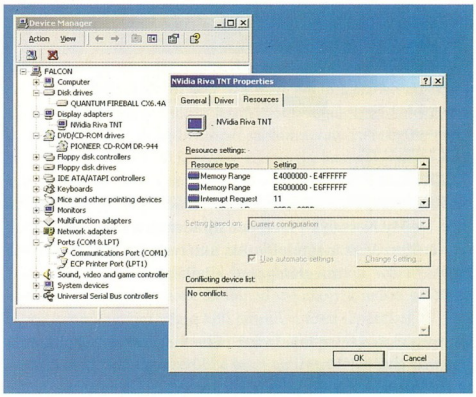
A hálózatok exponenciális növekedése megnövelte ugyan az üzleti felhasználó által rendelkezésre bocsátható és elérhető információ mennyiségét, ámde a rendelkezésre álló hatalmas adattömeg gyakran nagyon megnehezíti egy-egy konkrét dokumentum, mappa vagy erőforrás meglelését. Lássuk, a Windows 2000 e küldetésben hogyan szegődik segédünkül:

• **Általános keresés**

Nemcsak saját számítógépünkön, hanem a vállalati hálózaton, a vállalati intraneten és az Interneten is kereshetünk az egységesített *Keresés* (*Search*) eszközzel (ez a My Computerből, az Explorerből és a Start Menüből egyaránt elérhető).

A nemrég felkeresett hálózati helyek is egyszerűbben kereshetők (lásd a „My Network Places" bekezdést A továbbfejlesztett Asztal című részben). A keresés használja az AutoComplete funkciót is.

Az Active Directory címtárszolgáltatásokat használó Windows 2000 környezetekben gyorsan és hatékonyan kereshetünk a szervezethez tartozó személyeket, alkalmazásokat és hardvererőforrásokat is.



A hardvereket a Windows 98-éhoz hasonló könnyedséggel kezelhetjük

Az Active Directoryval például a rendszergazda úgynevezett globális katalógust (Global Catalog) is létrehozhat a felhasználó számára, amelyben az erőforrások listája optimalizált index formájában található meg.

A Windows 2000 a file-okat indexelni is tudja, ez azt jelenti, hogy egy háttérben futó program (a findfast) időről időre végignézi a gépen található összes file tartalmát, és néhány jellemző kulcsszó alapján „tárgymutatót" készít róluk. Az indexben sokkal gyorsabban meg lehet találni a keresett file-t, mintha végig kellene nézni valamennyi meghajtót (gondoljunk csak a könyvek tartalomjegyzékére).

• **Keresés az Interneten**

A Windows 2000 több úton is segíti az internetes keresést. A továbbfejlesztett Search panel a keresési lehetőségeket nem keresőgépenként (search engine), hanem témánként – webhelyek, emberek, vállalatok, térképek – jeleníti meg. A felhasználók és a rendszergazdák testre szabhatják az egyes témákhoz használt keresőket, sőt akár egyedi keresőrendszereket is megadhatnak. Ha az első keresőgépen nem járunk sikerrel, a *Next* gomb megnyomásával ugyanazt a kérdést másik rendszernek is feladhatjuk.

Ha a böngésző címsorán keresztül keresünk (például beírjuk, hogy Microsoft, ? Microsoft, vagy Go Microsoft), a szokásos listán kívül kiemelt tippet is kapunk, ha a rendszer talál ilyet.

• **Nyomtatók keresése**

Az Active Directory segítségével az általunk megadott feltételeknek (lapméret, kétoldalas nyomtatás, felbontás, szín) megfelelő nyomtatót is kereshetünk.

A különböző file-típusok kezelése

A legtöbb felhasználó számos különböző file-típussal dolgozik, különösen akkor, ha e-mail mellékleteket is kap.

A Windows 2000 fejlesztései jelentősen egyszerűbbé teszik a különböző file-típusok kezelését.

• **Az *Open With* funkció**

Gyakran előfordul, hogy a felhasználók olyan file-t kapnak, amelyről nem tudják, hogyan kell megnyitni; ez leggyakrabban az e-mail mellékletekkel fordul elő. A Windows 2000 továbbfejlesztett Open With funkciója egyszerűbbé teszi az ismeretlen típusú file-ok megnyitását. A file-ra az egér jobb gombjával kattintva megnyílik az Open With menü, amelyben a felhasználó az összes olyan regisztrált alkalmazásból választhat, amely az adott file-t meg tudja nyitni. Ha a file-t olyan alkalmazással akarja megnyitni, amely nem szerepel az Open With menüben, az *Any Program* elem választásával elindíthatja a továbbfejlesztett Open With párbeszédpanelt. Ebben a igénybe vehető alkalmazások és azok hagyományos ikonjai jelennek meg, így könnyen eldönthető, hogy melyiket kell használni. Miután a felhasználó adott alkalmazással megnyitotta a file-t, az Open With menü attól kezdve azt az alkalmazást is megjeleníti lehetőségként.

• **Automatikus alkalmazástelepítés**

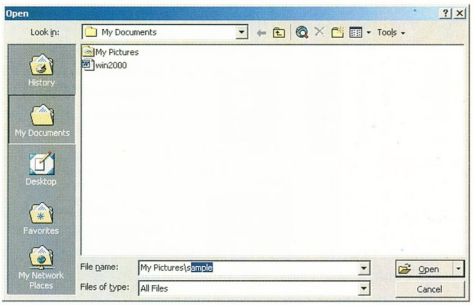
Az Active Directory címtárszolgáltatást használó Windows 2000 környezetben általában nincs szükség az Open With használatára.

A rendszergazda beállíthatja úgy a Windows 2000-et, hogy az automatikusan telepítse a Wordöt, ha valamelyik felhasználó például Word dokumentumot akar megnyitni.

Munka a hálózat leállása során

Becslések szerint a vállalatok több mint felében a felhasználóknak hálózati helyre kell elmenteniük a dokumentumaikat. Bár ez a szabály megkönnyíti a rendszergazdák számára a felhasználók dokumentumainak biztonsági mentését, azonban van egy nagy hátránya – ha a hálózat nem működik, a dokumentumok sem érhetők el.

E kellemetlenségre a Windows 2000 *Synchronization Manager* funkciója jelent gyógyírt. Az egér jobb gombjával adott dokumentumra vagy mappára kattintva és a *Make Available Offline*-t bejelölve az adott dokumentum vagy mappa mind a felhasználó számítógépén, mind a hálózati kiszolgálón tárolódik. A Synchronization Managerrel beállíthatjuk úgy a rendszert, hogy az elemeket a rendszer holtidejében, a felhasználó bejelentkezése vagy kijelentkezése során szinkronizálja. Mivel ekkor csak a változtatások másolódnak át, ezek a műveletek nem növelik meg jelentősen a hálózat forgalmát. Ha a hálózat leáll, a felhasználó nem veszi észre a kapcsolat hiányát. Amikor a hálózat ismét használhatóvá válik, a felhasználók üzenetet kapnak, hogy szinkronizálják a file-okat (ezt a funkciót *A Windows 2000 újításai noteszgépes felhasználóknak* című cikk részletesebben is boncolgatja).



A megújult Open/Save párbeszédpanel az Előzményeket és az AutoComplete-et is támogatja

Más fontos fejlesztések

• **A *Megnyitás/mentés* (*Open/Save*) párbeszédpanel**

Az új Open/Save párbeszédpanel egyszerűbbé teszi a dokumentumok megkeresését. Az Outlook stílusú eszköztár tartalmazza a felhasználó leggyakrabban használt dokumentumainak felsorolását és az *Előzményeket* (*History*). Az Open/Save használja az AutoComplete funkciót, és támogatja a miniatűröket (thumbnail).

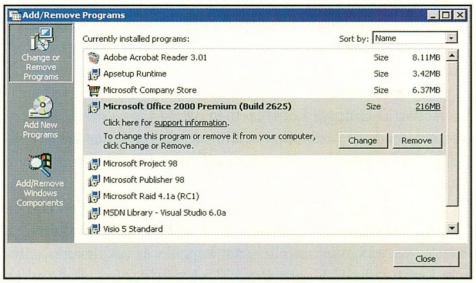
• **Internetes nyomtatás**

Az Internet Printing Protocol (IPP) használatával az Interneten keresztül is lehet nyomtatni feltéve, hogy a printer Windows 2000 Serverhez csatlakozik. Ez egyszerű és vonzó alternatíva a faxok és e-mail mellékletek helyett.

A beállítások megváltoztatása és a hibaelhárítás

A Windows 2000 fejlesztései jelentősen egyszerűbbé teszik az alkalmazások telepítését és a beállítások módosítását.

A *Programok hozzáadása Varázsló* (*Add/Remove Programs Wizard*) több információt nyújt az alkalmazásokról.



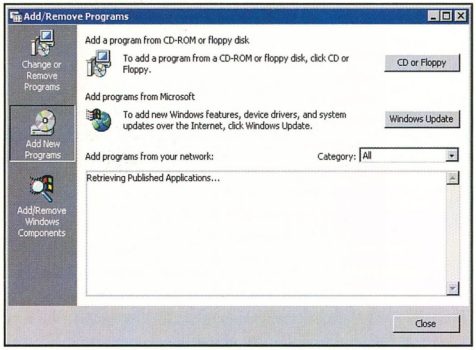
A továbbfejlesztett Add/Remove Programs több információt nyújt az alkalmazásokról

A *Windows Telepítő* (*Windows Installer*) technológiával önjavító alkalmazások készíthetők. A plug and play, az energiagazdálkodás és a Universal Serial Bus (USB) támogatása jelentősen egyszerűbbé teszi a hardverek kezelését. A továbbfejlesztett *Vezérlőpult* (*Control Panel*) logikusabban rendszerezi az eszközöket.

Az alkalmazások kezelése

A *Programok hozzáadása* (*Add/Remove Programs*, ARP) panel a korábbi változatnál lényegesen informatívabb: megtudhatjuk tőle, hogy az alkalmazás mekkora merevlemez-területet használ, hányas a verziószáma, milyen gyakran használjuk, valamint azt is, hogy van-e hozzá online ügyfélszolgálat. A Windows Installer technológiát használó alkalmazásokat a megfelelő gomb lenyomásával javítani is tudjuk a panelből, ekkor az alkalmazás változatlan beállításokkal újratelepíthető (ami reményhetőleg megoldja a gondot).

Ha vállalatunknál szoftvereloszto rendszer (pl.: Microsoft's System Management Server) is üzemel, az általunk elérhető alkalmazások automatikusan megjelennek az *Add Programs* párbeszédpanelben, így nem kell kézzel megkeresni az őket rejtő hálózati share-eket.



A házirend alapján telepíthető programok közül is választhatunk az Add New Programs panelen

Active Directorys környezetben az *Add New Programs* panelen a rendszergazda által felállított házirend alapján telepíthető alkalmazások automatikusan megjelennek (lásd még a *Group Policy a Windows 2000-ben* című cikkünket). Ha például a vállalat rendszergazdája hozzáférést enged a Visióhoz, a vállalat Windows 2000-et alkalmazó felhasználói telepíthetik a Visiót, vagy ha Visio mellékletet kapnak, az alkalmazás automatikusan telepítődik (lásd A különböző file-típusok kezelése című részt).

A rendszergazdák úgy változtathatják meg az alkalmazás-

A Windows 2000 Professional Vezérlőpultját úgy szervezték, hogy egyszerűbbé tegye a gyakori karbantartási feladtok elvégzését és a hibaelhárítást

elosztási pontot, hogy az semmilyen negatív hatást nem gyakorol az alkalmazás telepíthetőségére.

A hardverkezelés

A Windows 2000 hardvertámogatása sokkal jobb az NT-énél, támogatja a plug and playt, az energiagazdálkodást (ACPI-val) és a USB-t (Univerzális Soros Busz). Az USB-re egyszerűen rákapcsolhatjuk a legkülönfélébb perifériákat a billentyűzettől a fényképezőgépeken át a szkennerekig és egyéb képkezelő eszközökig (lásd még a *A Windows 2000 újításai noteszgépes felhasználóknak* című cikket).

Ha valamilyen okból a plug and play nem konfigurálja tökéletesen a hardvereszközöket, az *Add/Remove Hardware* varázsló segít a hibaelhárításban egyrészt a pillanatnyi beállítások megjelenítésével, másrészt hasznos tanácsokkal.

A Windows 2000 a telepítés előtt azt is ellenőrzi, hogy az eszköz meghajtóprogramja rendelkezik-e a hivatalos bevizsgálást bizonyító elektronikus aláírással. Ezáltal a felhasználók biztosak lehetnek benne, hogy eredeti forrásból származó, kipróbált meghajtóprogramot telepítenek, amely bizonyosan nem veszélyezteti rendszerük stabilitását (lásd a *Megbízhatóság – felsőbb szinten* című cikkünket).

A Windows 2000 CD-n levő összes driver rendelkezik a Microsoft aláírásával.

Az átszervezett Vezérlőpult (Control Panel)

A Windows 2000 *Vezérlőpultja* jelentős átszervezésen ment keresztül azért, hogy a felhasználók egyszerűbben végezhessék el a mindennapos karbantartási feladatokat, valamint a hibaelhárítást. E módosítások együttal a felhasználókat is védik attól, hogy olyan változtatásokat hajtsanak végre, amelyek a rendszer hibás működéséhez vezethetnek. Az alábbiakban a Vezérlőpult néhány fontos fejlesztését mutatjuk be.

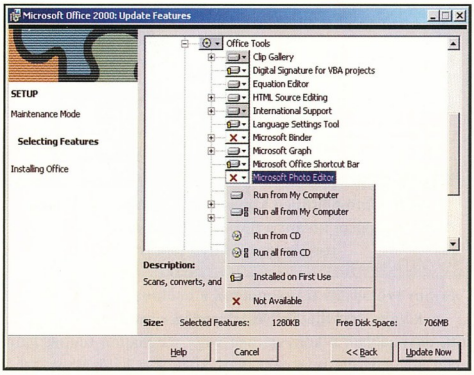
• **Logikusabb elrendezés:**
Ha a modemmel van gond, a *Modem* beállításai menüben a *Hardware* fület választva eljuthatunk a hibaelhárításhoz (Troubleshoot).

• **Rendszer (*System*):**
Több alkalmazás kombinálásával egyszerűbbé teszi a rendszer beállítását: *Network Identification*, *Hardware*, *User Profiles* és *Advanced*.

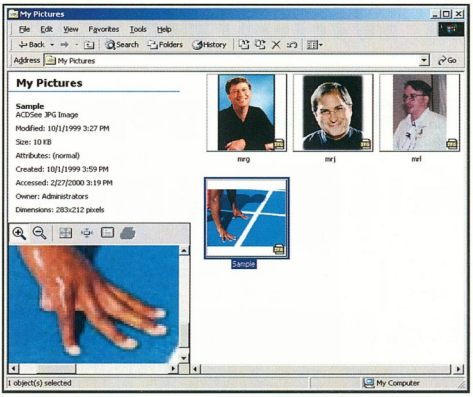
• **Felhasználók és jelszavak (*Users and Passwords*):**
Ezzel az alkalmazással felhasználókat és csoportokat adhatunk a rendszerhez. Ha adminisztrációs jogokkal nem bíró felhasználó indítja el, akkor a korábbi Windowsok viselkedése helyett – ezek rövid hibaüzenet után kiléptek – lehetőséget ad rendszergazda-szintű felhasználó nevének és jelszavának megadására. Ezáltal a rendszergazda a nélkül tudja konfigurálni a jogokat, hogy előbb ki kellene léptetni a gép felhasználóját, utána pedig vissza.

• **Mappabeállítások:**
Megváltoztathatjuk az *Asztal* és a mappák megjelenési módját. Például eldönthetjük, hogy a mappák ugyanabban, vagy külön-külön ablakokban nyíljanak meg. Azt is meghatározhatjuk, hogy a megnyitáshoz az egyetlen kattintás elegendő legyen, vagy kettőt kelljen klikkelni.

• **Új hardver hozzáadása (*Add/Remove Hardware*):**
Ezzel a központi varázslóval a felhasználók hardverelemeket adhatnak a rendszerhez, eltávolíthatják azokat, vagy elháríthatják az esetleges hibákat. Ha a Windows 2000 új hardvert ismer fel, ellenőrzi az eszköz beállításait, és telepíti a megfelelő meghajtót.
A varázsló a már telepített hardverelemek listáját is megjeleníti, és segít a felhasználónak ellenőrizni, hogy az eszközök megfelelően működnek-e.



Az új telepítő lehetővé teszi, hogy a ritkán használt részek első használatkor automatikusan installálódjanak



A My Pictures mappa egy igazi képnézegetővé fejlődött

• **Adminisztrációs eszközök:**
Az NT-ben még a Programok közé rejtett *Administrative Tools* mappa átkerült a vezérlőpultra. A benne található eszközök elsősorban a rendszergazdának szólnak, az átlagos felhasználók számára szükségtelenek.

•• Component Services:
A rendszergazda ezzel az eszközzel grafikus felületen telepítheti és adminisztrálhatja a COM+ programokat, valamint az adminisztratív feladatokat automatizáló scripteket vagy programokat készíthet.

•• Computer Management:
A rendszergazda ezt az eszközt arra használja, hogy helyi vagy távoli számítógépeket kezeljen egységes segédprogram segítségével. A Computer Management a Windows 2000 több adminisztrációs eszközét (*System Tools*, *Storage*, *Server Applications* és *Services*) egyetlen konzolfává kombinálja, ezáltal valamennyi adminisztrációs terület egyszerűen elérhető.

•• Data Source (ODBC):
A kapcsolatközösítés (*Connection Pooling*) lehetővé teszi, hogy az alkalmazások újrahasznosítsák a nyitott kapcsolatokat, és ne kelljen mindig újak nyitásával vesztegetni az erőforrásokat.

•• Event Viewer:
Ez az eszköz az eseménynaplót szöveges file-ba exportálja.

Összegzés

A mindennapi felhasználók akkor tudnak a leghatékonyabban dolgozni, ha tisztában vannak a számítógép és az operációs rendszer használatával. A hatékonyan használt számítógép és operációs rendszer megéri az árát, mivel segít felhasználója munkáját hatékonyabbá varázsolni.

A Windows 2000 újításai a noteszgépes felhasználóknak

A Windows 2000 Professional a hordozható gépek felhasználóinak is rengeteg újítással kedveskedik. Ezek segítségével a felhasználók egységesebb, könnyebben kezelhető és biztonságosabb munkakörnyezetet hozhatnak létre mind utazás közben, mind pedig az irodában.

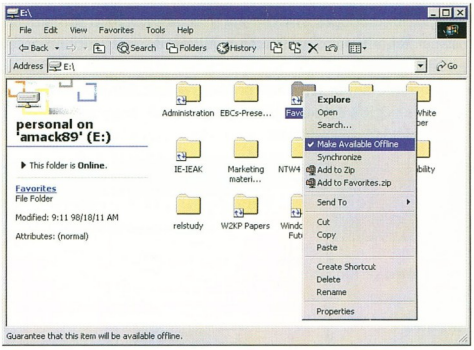
A noteszgépes funkciók kifejlesztése során az volt a fő cél, hogy a felhasználó ugyanúgy használhassa gépét utazás közben, mint az irodai asztalánál. Ennek elősegítésére a Windows 2000 a hálózaton található file-okról naprakész másolatokat tart fenn, gondosabban ügyel adataink biztonságára, jobban takarékoskodik az akkumulátorral, mindemellett még a távoli kapcsolatok konfigurálását is leegyszerűsíti. De a további hozsannák helyett lássuk a részleteket!

Zsebre vágott adatok

A fent említett file-szinkronizálás lehetővé teszi, hogy a felhasználók menet közben ugyanúgy dolgozzanak a hálózaton található állományokkal, mint ahogy a vállalati hálózathoz csatlakoztatva tennék. Ezáltal hatékonyabbá válhat munkájuk, ugyanis anélkül használhatják gépüket az irodán kívül, hogy indulás előtt mindig oda kellene figyelniük a megfelelő file-ok gondos ide-oda másolgatására.

File-ok és mappák elérése kapcsolat nélkül

A korábbi Windowsokból megismert *Briefcase* (*Táska*) helyét sokkal kényelmesebben használható és sokkal rugalmasabb újdonság vette át. A *Make available offline* (*legyen elérhető kapcsolat nélkül*) funkció segítségével aktív hálózati kapcsolat nélkül is hozzáférhetünk leggyakrabban használt file-jaink, mappáink vagy akár teljes hálózati meghajtóink tartalmához (az egyetlen korlátozás, hogy ezeknek Windows vagy SMB-kompatibilis szerveren kell lennie). Használatához elegendő az adott hálózati erőforrás nevére kattintani az egér jobb gombjával, majd a megjelenő menüből kiválasztani a *Make available offline* menüpontot. (A *Windows 2000 – az új gazdaság alapja* című cikkünkben e lehetőség még egy érdekes felhasználását említjük: vándorló profilok nélkül is áthelyezhetjük a *My Documents* mappát a szerverre.)

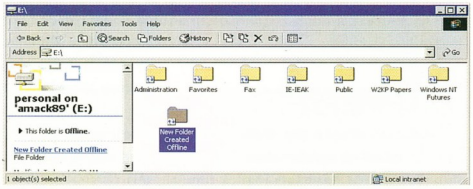


A jobb gombmenüben kijelölhetjük a kapcsolat nélkül elérni kívánt a file-okat és mappákat (ezeket kettős nyíl jelöli)

A kiválasztott file-okat és mappákat ezután mindig ugyanott, ugyanabban a könyvtárban vagy meghajtón fogjuk látni, még akkor is, ha már nem csatlakozunk a hálózathoz, tehát pont úgy használhatjuk őket, mintha még mindig az irodában ülnénk. Az egyetlen árulkodó jel, hogy a kijelölt mappa vagy file ikonjának bal alsó sarkában kettős nyíl látható (érdekes-

ségképpen: ezt a Microsoft terminológia roundtrip, azaz retúrnyílnak nevezi).

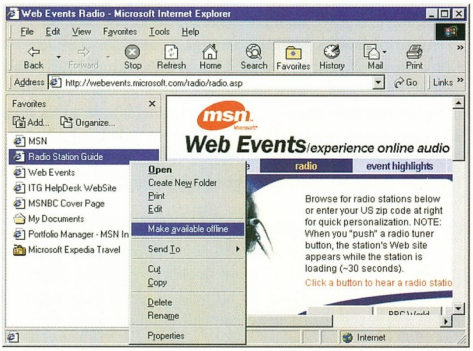
A fenti szolgáltatás párja a Windows 2000 Serverben is megtalálható: az adminisztrátor beállíthatja, hogy melyik mappák tartalmát szabad a helyi gépeken tárolni, azaz megtilthatja a biztonsági szempontból érzékeny anyagok széthordását.



A file-ok és mappák pont úgy használhatók, mintha a hálózati kapcsolat aktív lenne. Az offline végzett módosítások a kapcsolódás után automatikusan szinkronizálódnak

Webtartalom elérése kapcsolat nélkül

Honlapokat vagy teljes webhelyeket is haza lehet vinni. Ehhez mindössze, hasonlóan a file-okhoz, a lap vagy hely címére kell kattintani az Internet Explorerben. A feladat annyival bonyolultabb, hogy a varázsló kérdéseire válaszolva be kell állítani, hogy pontosan mire is van szükségünk (az adott lapra vagy a kapcsolódó lapokra is), valamint hogy milyen gyakran szeretnénk frissíteni a helyi másolatot.



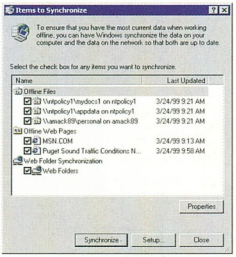
A file-okhoz hasonlóan a honlapokat is elérhetővé tudjuk tenni a kapcsolat nélküli időkre

A szinkronmester

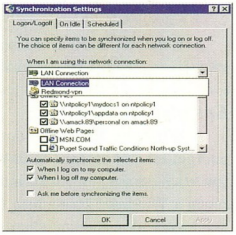
A korábbi operációs rendszerekben ha valaki kapcsolat nélkül szeretett volna dolgozni, gondos munkával minden fontos anyagot külön-külön le kellett másolnia a gépére, az e-mailektől a naptárán keresztül az adatbázisokig. Amikor pedig visszaért az irodába, a megváltozott adatokat vissza kellett másolnia a szerverekre. Ez a szinkronizáció nem volt egyszerű feladat, ámde mostantól nem is kell kézzel végeznünk...

Szinkronizáció Menedzser

A *Synchronization Manager (Szinkronizáció felügyelet)* eszközzel központilag állíthatjuk be, hogy melyik file-okat szeretnénk szinkronizálni, és hogyan. Például megadhatjuk, hogy bizonyos file-okat vagy mappákat minden hálózati bejelentkezés során szinkronizálni szeretnénk, ennek hatására a következő alkalommal a program gyorsan végignézi a rendszert, és ha változást talál, automatikusan frissít. Nemcsak a be- és kilépéskorra, hanem adott időpontokra vagy a kihasználatlan (idle) időszakokra is kérhetjük a frissítést. A folyamat aránylag gyors, ugyanis a rendszer csak a megváltozott állományokat másolja át.



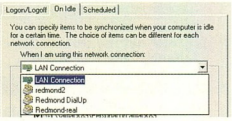
A Synchronization Managerrel központilag frissíthetjük az offline file-okat



Bejelentkezéskor vagy egyedi időpontokban is szinkronizálhatunk

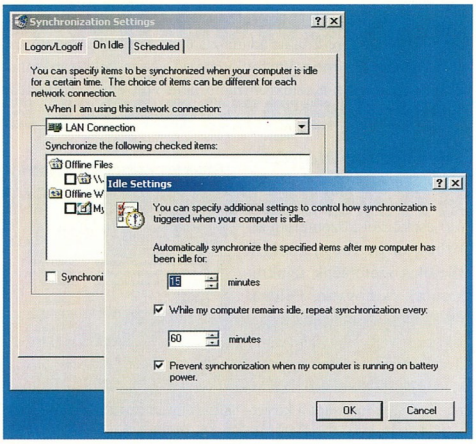
Kapcsolatok szerint is beállíthatjuk a menedzsert, például beállítható, hogy a nagy adatbázisokat csak nagy sebességű kapcsolaton (helyi hálózat) próbálja frissíteni, a személyes dokumentumokat viszont minden adandó alkalommal.

Az új szolgáltatásnak köszönhetően elég egyszer beállítani, hogy mikor melyik file-okra van szükségünk, és soha többet nem kell amiatt aggódnunk, hogy épp a legfontosabb dokumentumot felejtettük el lemásolni indulás előtt. Bár a Szinkronizáció Felügyelet elsődleges feladata a dokumentumok frissítése, abban is segít, hogy megoldjuk a verziókonfliktusokat, mikor adott file-t több ember változtat meg párhuzamosan.



Az adatok egyéni fontossági sorrend szerint frissíthetők

A Microsoft a Synchronization Managerhez programozói felületet (API) is ké-



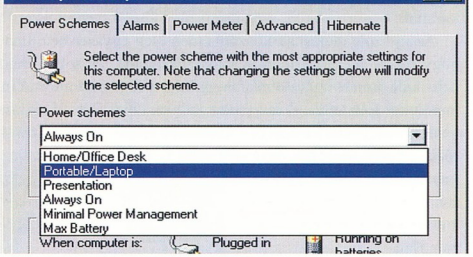
szített, így az első szinkronizációra felkészített levelező- és irodai programok valószínűleg hamarosan megjelennek.

Csak megy, csak megy, csak megy

A Windows 2000 újításainak köszönhetően a lehető legtovább használhatjuk masinánkat út közben.

Energiagazdálkodás

A Windows 2000 a hordozható gépek esetében oly fontos energia-takarékosságra is ügyel a legfejlettebb energia-felügyeleti módszer, az ACPI interfész támogatásával. Az ACPI révén a Windows 2000 „meg tudja kérdezni" a felhasználó, az alkalmazások, valamint a hardvereszközök igényeit, és ez alapján tudja szabályozni a gép pillanatnyi állapotát. Például az a felhasználó, aki sok telefonhívást bonyolít, és közben időnként noteszgépe segítségével jegyzeteket készít, beállíthatja a rendszert úgy, hogy az két percnyi tétlenség után kapcsolja ki a képernyőt és a merevlemezt, öt perc után pedig kerüljön készenléti (Standby) állapotba. Így a gép ugyan lassabban használható – hiszen mindig meg kell várni, hogy feléledjen –, cserébe viszont az akkumulátor egyetlen töltéssel akár egész nap kitart. Tehát csak a felhasználón múlik, hogy a nagyobb sebességet vagy a kisebb fogyasztást választja-e.



A többféle energiagazdálkodási beállítás lehetővé teszi, hogy megtaláljuk a legjobb kompromisszumot a teljesítmény és az akku élettartama között

De nemcsak a felhasználó, hanem a futó alkalmazások is jelezhetik igényüket. A sokáig tartó számolást (például filmlejátszást) végző programok értesíthetik az operációs rendszert, hogy ne kapcsoljon alacsony energiafogyasztású állapotba. Ez visszafelé is működik, az operációs rendszer tudathatja az alkalmazással, hogy a gép éppen akkuról üzemel, ennek hatására az „udvarias" program lehetőleg máskor végzi az áramfalóbb műveleteket (például az e-mailek tömörítését).

Az eszközinterfész segítségével a rendszer a hardvereszközök eseményeit is kezelni tudja. Vegyünk egy mobiltelefonhoz csatlakozó modemmel is rendelkező gépet. Ezt például vonatút során faxüzemmódba lehet kapcsolni, ezáltal csak a modem fogyaszt némi energiát. Ha hívás érkezik, a modem bekapcsolja a gépet, fogadja a hívást, és letölti a faxot. Foglalatossága végeztével a gép megint kikapcsol, így csak a valóban szükséges mennyiségű energiát fogyasztja.

Eszközök csatlakoztatása és felügyelete

A Windows 2000 támogatja a plug and playt, sőt noteszgépek esetén a legtöbb kártyát újraindítás nélkül telepíthetjük. Ezzel sok időt spórolhatunk meg, ami például prezentáció során a projektor csatlakoztatásakor nagyon jól jöhet. Érdekesség, hogy az ACPI támogatásnak köszönhetően a Windows 2000 plug and playe stabilabb a korábbi Windowsokénál.

Az új operációs rendszer támogatja az USB (Univerzális Soros Busz) eszközöket is, ezeket szintén újraindítás nélkül csatlakoztathatjuk. Az USB előnye, hogy az összes periféria ugyanolyan kábelt használ, azaz nem kell teletömni a táskánkat fél tucat különféle csatlakozóval és dróttal. Ráadásul a legtöbb USB-s eszköz a számítógéptől kapja az áramot, így a tápkábelektől és tápegységektől is megszabadulhatunk.

Dokkoló állomások használata

A Windows 2000 megengedi, hogy újraindítás nélkül csatlakoztassuk, és vegyük le a hot docking szabványt támogató gépeket a dokkoló egységről. Ez például akkor nagy segítség, mikor egy megbeszélés erejéig át kell vinni gépünket az irodából a konferenciaterembe.

Hardverprofilok

NT 4 alatt kézzel kellett beállítani a hardverprofilokat, és minden indításkor ki kellett választani a megfelelőt.

A Windows 2000 tulajdonosai ellenben könnyen használhatják különböző konfigurációkban rendszerüket anélkül, hogy az eszközöket mindig újra be kellene állítaniuk, vagy az adott

profilban nem szereplő eszközök hibaüzeneteire kellene figyelniük.

A különböző környezetekhez egyedi beállításokat használhatunk

OnNow: Gyors indítás és Leállás

Az átlagos számítógépek elindulása akár több percig is eltarthat – ez túl sok idő a fontos üzleti tárgyaláson, amikor az asztal túloldalán a türelmetlen potenciális ügyfelek várakoznak a válszra várva.

A Windows 2000 ACPI támogatása lehetővé teszi, hogy a gép tényleg szinte egyetlen gombnyomásra induljon, ugyanis *Hibernált* üzemmódból kevesebb, mint fél perc alatt el lehet indítani. A hibernáció azt jelenti, hogy a futó programokat és az eszközök állapotát a gép merevlemezre menti, és kikapcsol. A bekapcsolás után ott folytathatjuk a munkát, ahol abbahagytuk. A masina még gyorsabban, pár másodperc alatt magához tér a *Felfüggesztett* (Suspend) üzemmódból, melyben nem kapcsol ki teljesen, csak mély álomba merül. Ennek persze ára van, a felfüggesztett gép ha lassan is, de meríti az akkumulátort. Ám így is órákat nyerhetünk.

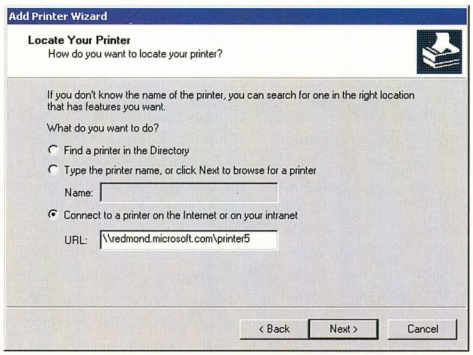
A hibernált és a felfüggesztett üzemmódok használatával elkerülhetjük a rendszer időigényes teljes újraindítását

Internetes nyomtatás

Az új rendszer lehetővé teszi, hogy az Interneten keresztül nyomtassunk. Ez jól jöhet például egy szállodában, ahol ezáltal nem kell elballagnunk a nyomtatóig, vagy különböző meghajtóprogramokkal és kábelekkel foglalkoznunk.

Az nyomtatáshoz mindössze a nyomtató helyét kell megadnunk. A szükséges meghajtóprogramok automatikusan települnek az Interneten keresztül, és már kezdhetjük is a nyomtatást. A szerver olyan weblapot is automatikusan létrehoz, ahol böngészőnkkel figyelemmel kísérhetjük a nyomtató és a nyomtatási munkák állapotát.

A szerveroldalon azonban Windows 2000 Server szükséges az internetes nyomtatómegosztáshoz.



Az Interneten keresztül is tudunk nyomtatni

Bedrótozva

Mint a bevezetőben említettük, a hálózati- és távoli kapcsolatok konfigurálása is sokkal kényelmesebb az új operációs rendszerben.

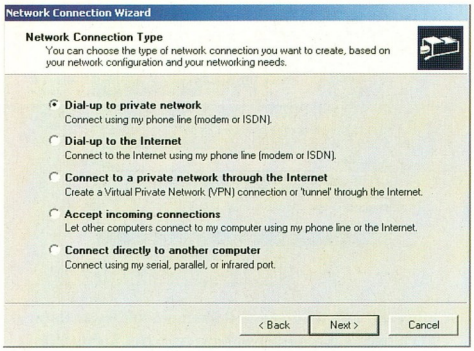
Távoli kapcsolatok létrehozása

Könnyebben hozhatunk létre modemes kapcsolatokat vagy virtuális magánhálózatot (VPN), és egyszerűbbé vált a gépek összekötése infravörös porton vagy közvetlen kábelkapcsolattal is.

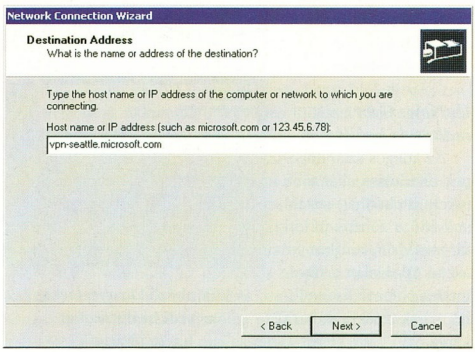
Megmenekülhetünk a kézi beállítgatástól, ugyanis varázsló segít a különböző csatlakozások létrehozásában és telepítésében (ez az összes szükséges szervizt is telepíti, így nem kell a hálózati beállításokban kotorászni, mint a Windows 95 esetében).

A következő újításokkal találkozhatunk a varázsló által felajánlott kapcsolattípusok között:

- **Telefonos bejelentkezés privát hálózatokra:** továbbfejlesztették a hívókártyák, PIN-kódok és egyéb kapcsolat-specifikus jellemzők kezelését.
- **Telefonos Internet-kapcsolat:** pontosabban beállíthatjuk a proxy- és egyéb Internet-specifikus beállításokat.
- **Virtuális magánhálózatok elérése az Interneten keresztül:** újraindítás nélkül csatlakozhatunk a VPN-ekhez.
- **Bejövő hívások fogadása:** az új rendszerben pontos elérési jogokat adhatunk meg a modemen, infravörös porton vagy a közvetlen kábelkapcsolaton keresztül becsatlakozó felhasználóknak.



Egy helyen hozhatjuk létre a kapcsolatok minden fajtáját



Csak a VPN kiszolgáló nevét kell megadnunk, és a kapcsolat máris kész

• **Közvetlen kapcsolódás másik számítógéphez:** a varázsló már a kábelkapcsolat konfigurálásában is segít.

Virtuális magánhálózatok

A Virtuális magánhálózatok (VPN) lehetővé teszik, hogy a felhasználók biztonságos csatornát alakítsanak ki az Interneten keresztül vállalatuk helyi hálózatához (LAN). Ahhoz, hogy ez létrejöhessen, a felhasználónak először csatlakoznia kell az Internethez (ezt szinte bármilyen módon megteheti, például a helyi szolgáltató segítségével is), majd pedig a kapcsolat „felett" el kell indítania a VPN csatlakozást. A VPN fő előnye a közvetlen betárcsázással szemben, hogy segítségével meg lehet takarítani a távolsági hívások díját anélkül, hogy feláldoznánk a vállalati LAN biztonságát.

A VPN konfigurálásához csak meg kell adni a cégünknél üzemelő VPN-szerver nevét, a szükséges eszközök és hálózati szolgáltatások telepítése már a varázsló dolga.

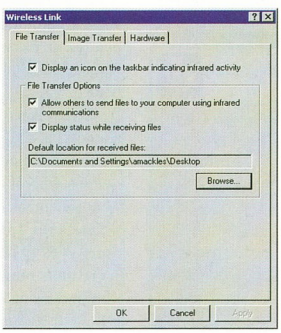
A jelenleg legelterjedtebb VPN protokoll, a Point-to-Point Tunneling Protocol (PPTP) mellett a Windows 2000 Professional támogatja a virtuális kapcsolatok új, biztonságosabb módszereit is, köztük a Layer-2 Tunneling Protocolt (L2TP) és az IP Securityt (IPSec).

Drótnélküli Kapcsolatok

A Windows 2000 támogatja az infravörös adatátvitelt megvalósító IrDA protokollt, így a felhasználó fizikai kábelkapcsolat nélkül elérhet adatokat és megosztott erőforrásokat (pl.: nyomtatókat) másik gépen is. Az IrDA rendszer automatikusan felépíti a kapcsolatot, amint a két gép eléggé közel kerül egymáshoz. A legtöbb új hordozható számítógépnek van már IrDA portja.

Az IrDA kapcsolat kiválóan használható például akkor, ha csak gyorsan ki szeretnénk nyomtatni valamit a noteszgépünkről. Elég odasétálni valamelyik a nyomtatóhoz – hálózaton vagy helyileg – csatlakozó számítógéphez, és (a megfelelő jogosultságok birtokában) drótok dugdosása nélkül máris nyomtathatunk.

A Windows 2000 azt is lehetővé teszi, hogy az általunk meghatalmazott felhasználók file-okat küldjenek az infra porton keresztül. A bejövő állományokat a rendszer az általunk megadott mappába teszi. A rendszer nemcsak a többi gépet, hanem az IrDA kapcsolatra képes eszközöket (pl.: digitális fényképezőgép) is felismeri.

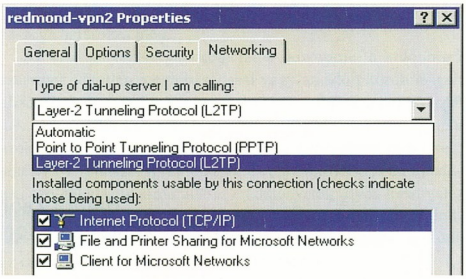


A Windows 2000 natív támogatást nyújt az infravörös kommunikációhoz

Egy eszköz használata több kapcsolatra

A hordozható gépek tulajdonosai rendszerint több különböző hálózathoz csatlakoznak utazásaik során, a vállalati helyi hálózattól a különféle helyi Internet-szolgáltatókig. A Windows 95 és az NT 4.0 esetében a modem beállításai közösek voltak, az az mindegyik kapcsolatra vonatkoztak, így ha a felhasználó felváltva használt különféle modembeállítást igénylő rendszereket, akkor vagy folyton váltogatnia kellett a beállításokat, vagy seregnyi „virtuális modemet" kellett létrehoznia és karbantartania.

Az új Kapcsolatalapú (Per-connection) filozófia az összes hálózati kapcsolathoz külön nyilvántartja az eszközök beállításait,



Több különböző beállítás rendelhető ugyanahhoz az eszközhöz

így a felhasználó anélkül csatlakozhat több különböző hálózathoz, hogy mindegyikhez észben kellene tartania a szükséges beállításokat.

Elrejtett információ

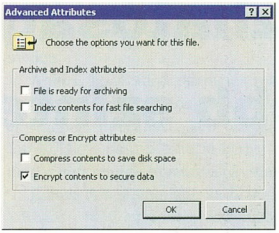
Utazás közben előfordulhat, hogy a hordozható számítógépet ellopják. A Windows 2000 lehetővé teszi, hogy ez ne okozzon katasztrofális károkat. (Mint a fentiekben láthattuk, az új rendszer a másik fő veszélyforrást, az internetes adatcserét is segít biztonságosabbá tenni.)

Adatvédelem

Az EFS Titkosított File-rendszer révén rejtjelezhetjük a noteszgépen található, érzékeny információt tartalmazó file-okat. Ha a gépet ellopják, az EFS még akkor is megvédi az adatokat, ha „új tulajdonosa" újratelepíti a Windowst.

(Az EFS technológiáról további részletek olvashatók a Hitelesség 2000 után és *A Windows 2000 biztonsági szolgáltatásai* című cikkekben).

Ha a kiszolgálón Windows 2000 Server, a munkaállomá-



Az EFS lehetővé teszi adataink titkosítását

sokon pedig Windows 2000 Professional fut, a felhasználó a szerveren is titkosítva tárolhatja az adatait. Házirend-beállítás kérdése, hogy ezeket az állományokat csak a felhasználó, vagy a felhasználó és a rendszergazda is tudja-e dekódolni (ez utóbbi beállítás azért is praktikus, mert így az adatok nem vesznek el, ha a felhasználó távozik a cégtől, vagy elfelejti a jelszavát).

Felhasználói profilok

Sok cégnél egy hordozható gépet több alkalmazott is használ. A felhasználói profilok létrehozásával megakadályozhatjuk, hogy a felhasználók elolvassák egymás adatait. A rendszergazda döntheti el, hogy a felhasználók csak saját védett adatokkal, vagy saját alkalmazásokkal és a beállításokkal is rendelkezzenek-e. Csak a rendszergazda láthat minden adatot. Sok hardver – például a modemek és a hálózati kártyák – beállítható úgy, hogy valamennyi felhasználó elérhesse.

File-elérési jogosultságok

Az NT-s hagyományoknak megfelelően a felhasználók minden állományhoz hozzáférési jogosultságokat állíthatnak be helyben és a távolról bejelentkezve is. A jogosultságok felhasználókhoz vagy csoportokhoz köthetők. Például a felhasználó megadhatja, hogy adott mappa csak olvasásra vagy teljes körűen legyen elérhető mások számára. Ez hasznos, ha többen használják a gépet, és cserélhető eszközökre is alkalmazható, például PC-kártyán keresztül csatlakozó NTFS 5 file-rendszert használó merevlemezekre.

A hordozható számítógép védelme intelligens kártyával

A Windows 2000 támogatja a Smart Cardok használatát, ezekkel még nagyobb biztonságba helyezhetjük a hordozható gépen tárolt adatokat (a részleteket lásd *Hitelesség 2000 után a Smart Card alkalmazásával* című cikkünkben).

Mutatók

A PPTP, L2TP és IPSec szabványokról:

www.microsoft.com/windows2000/library/howitworks/security/ip_security.asp

www.microsoft.com/windows2000/library/howitworks/communications/remoteaccess/l2tp.asp

Megbízhatóság – felsőbb szinten

Bátorfi Zsolt
zbatorfi@microsoft.com

A Windows 2000 a Microsoft eddigi legterebélyesebb és – bár ez látszólag ellentmondás – legmegbízhatóbb operációs rendszere. A megbízható működés a rekordhosszúságú tesztelésnek és néhány régóta várt újításnak köszönhető.

A Windows 2000 operációs rendszercsalád kereskedelmi megjelenésével az informatikai ipar minden bizonnyal legnagyobb szoftverprojektje fejeződött be tavaly decemberben.

A fejlesztés méreteit jól érzékelteti, hogy közel nyolc évig tartott, a – Windows NT 4 architektúrából továbbfejlesztett – kód pedig időközben közel 30 millió sorra gyarapodott. További érdekesség, hogy a Microsoft nemcsak számtalan új szolgáltatással bővítette a korábbi rendszert, hanem a meglévő kódösszetevők több mint felét is újraírta vagy optimalizálta a stabilitás és a teljesítmény növelése céljából.

Mindezzel párhuzamosan – a Microsoft történetében szintén egyedülálló módon – a cég már a kezdeti fejlesztési fázisokban bevonta potenciális fejlesztői kapcsolatait, üzleti partnereit, valamint a nagyvállalati ügyfélbázisát a rendszer tesztelésébe és továbbfejlesztésébe.

A fentiek eredményeként számos független szakmai fórum szerint az augusztusban kiadott, funkcionálisan a végleges rendszerrel azonos béta 3-as változat a kereskedelmi forgalomban használt szoftverektől elvárt, sok tekintetben azt meghaladó módon megbízhatónak bizonyult.

A következő generációs operációs rendszer és a köré épülő platformszolgáltatások február 17-i hivatalos megjelenésével sokakban felvetődhet a kérdés: a népszerű hálózati operációs rendszer valójában milyen irányban fejlődik tovább, milyen új architekturális összetevőket tartalmaz majd, amelyek egyértelműen megkülönböztetik a Microsoft korábbi operációs rendszereitől (Windows 9x, NT4)?

Mindezzel párhuzamosan a rengeteg új funkció megjelenése, a mindenre kiterjedő teljesítmény-optimalizálás vajon milyen hatással van a rendszer általános stabilitására, röviden: a Windows 2000 mennyivel stabilabb rendszer, mint elődei, s melyek azok a szolgáltatások, amelyek ezt az alkalmazást a modern hálózati operációs rendszerek minőségileg magasabb kategóriájába helyezik?

A következőkben ezekre a kérdésekre próbálok választ keresni, miközben bemutatom azokat az új technológiákat és rendszerelemeket, amelyek a Windows 2000 megbízhatóságát meghatározzák.

Mit jelent a rendszerek megbízhatósága?

Több külföldi közvélemény-kutatás (www.survey.com), illetve rangos informatikai szaklapok (Windows NT Magazine), IT-döntéshozók, rendszeradminisztrátorok és fejlesztők visszajelzéseire támaszkodó felmérések alapján az operációs rendszerek minőségét – a felhasználók szemében – elsődlegesen a megbízhatósággal jellemzett tulajdonságuk határozza meg.

Sajnos a megbízhatóság nehezen mérhető fogalom, számos felhasználó és rendszeradminisztrátor ezért a szubjektív érzeteire, és – talán túl sokszor is – a felkészületlenségéből, valamint a technológiai félinformációkból építkező tévhiteire építi az erről alkotott képét.

Ezért mielőtt belemélyednénk a Windows 2000 megbízhatóságával kapcsolatos ismeretekbe, fontos tisztáznunk, valójában mit is jelent adott operációs rendszer megbízhatósága, s ténylegesen melyek azok az összetevők, amelyek a stabilitást befolyásolják.

A pontosság kedvéért: adott rendszer megbízhatóságát kizárólag annak előre nem látható leállásai (lefagyások), illetve a tervezett, valamilyen körülmény által szükségszerűvé vált leál-

lások következtében fellépő szolgáltatás-kimaradások idejének összege határozza meg.

Az első tényezőre (unpredictable downtime) a különböző szervizek váratlan meghibásodásai vagy az adott körülmények között bekövetkező teljes rendszerösszeomlások lehetnek példák. A második kategóriába (predictable downtime) tartoznak azok a frissítési vagy átkonfigurálással kapcsolatos helyzetek, amelyek a rendszer újraindítását, és ebből következően a hálózati szolgáltatások kimaradását eredményezik. Ilyen lehet valamelyik kritikus rendszerösszetevő – például a hálózati alrendszer (protocol stack) – telepítése vagy átkonfigurálása, ugyanis ez csak a rendszer újraindításával lehetséges.

És végül a teljesség kedvéért a megbízhatóságot szét kell választani az elérhetőség és a skálázhatóság által leírt jellemzőktől, ezek már másik tanulmány témakörébe tartoznak.

Az operációs rendszerek megbízhatóságát befolyásoló tényezők

Az operációs rendszerek megbízhatóságát elsősorban – a közhiedelemmel ellentétben – nem a rosszul megírt alkalmazások, a rendszert tesztelők előtt rejtve maradt belső hibák (bugok) vagy tervezésbeli hiányosságok veszélyeztetik.

A veszély ennél nagyságrendekkel bonyolultabb területen keresendő, nevezetesen azokban a hibákban, amelyek az operációs rendszer központi végrehajtó alrendszerével (System Executive) azonos privilegizált szinten futó eszközvezérlőkben – például képernyő-, hangkártya- vagy nyomtatóvezérlők – és a rendszerközeli szolgáltatásokban bújnak meg alattomos módon.

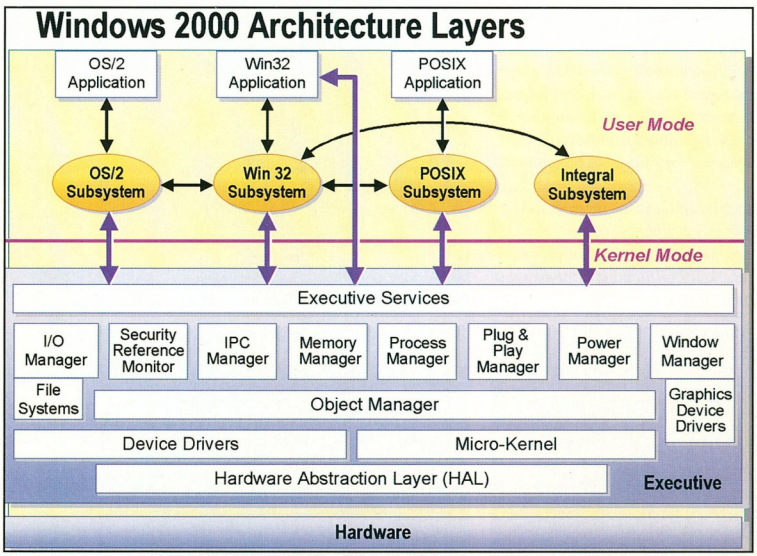
Ahhoz, hogy adott operációs rendszer hatékonyan működhessen, egyes külső összetevőknek is a központi maggal egyenrangú hozzáférést kell biztosítani az olyan kritikus erőforrásokhoz, mint például a kernel és az eszközvezérlők által megosztott rendszermemória (System Pool).

Ennek minél stabilabb és biztonságosabb megoldása örök kihívás – még az operációs rendszerek fejlődéstörténetében egyre kifinomultabbá váló időosztásos, mikrokernel architektúrában is. Amennyiben ezek a külső komponensek rossz tervezés, vagy hiányos tesztelés következményeként nem megfelelően élnek a „jogaikkal és kötelességeikkel", a rendszer bármely pillanatban instabillá válhat. A megbízhatósággal kapcsolatban ezért a fő kérdés az, hogy az operációs rendszer mennyire képes kezelni a vele azonos szinten futó külső összetevők váratlan hibáit.

A következőkben vizsgáljuk meg, hogy a Windows 2000 redmondi fejlesztőcsapata milyen célokat tűzött ki ezekkel kapcsolatban.

A Windows 2000 megbízhatóságát célzó fejlesztési irányvonalak

A Windows 2000 nem csupán operációs rendszer. A Microsoft ezt a szolgáltatásközpontú, elosztott komponenstechnológiákra épülő, következő generációs platformjának első, s egyben legfontosabb építőkövének szánta.



A Windows 2000 rendszerfelépítése

A Windows 2000 magja köré tervezett platform-szolgáltatások számára ezért a megbízhatóság meghatározó fontosságú. Így a fejlesztők az alábbi alapvető elvárásokat jelölték ki:

- az egyre összetettebb új funkciók (például Active Directory, plug and play, Terminal Server, fürtözési alrendszerek) ne ronthassák a rendszer általános megbízhatóságát;
- a telepített összetevők stabilitása ne befolyásolja az OS üzembiztosságát;
- a stabilitást veszélyeztető komponensek legyenek egyértelműen azonosíthatók, illetve kiiktathatók;

- a minőségileg bevizsgált eszközvezérlők (driverek) hitelessége ellenőrizhető legyen (digitális aláírásokkal);
- az aláírással nem bíró eszközvezérlők kizárhatók legyenek a házirend megfelelő beállításával;
- a rendszer átkonfigurálása a lehető legkevesebb újraindítással járjon;
- a kritikus rendszer- és alkalmazás-összetevők (pl.: Registry, DLL-ek) verziói központilag felügyelhetők legyenek;
- az alkalmazások teljes életciklusa kezelhetővé váljon az új, házirendalapú telepítő rendszer segítségével.

A Windows 2000 megbízhatóságával kapcsolatos új technológiák

A következőkben vizsgáljuk meg, hogy milyen kézzelfogható új technológiák bevezetésével sikerült elérni az előzőekben felsorolt fejlesztési célokat.

Az NT 4 esetében az adminisztrátor könnyen beleeshetett az alábbi csapdák egyikébe:

- *Az OS nem indítható újra*

  Bármely hibásan megírt eszközvezérlő, vagy rosszul konfigurált szerviz megakadályozhatja a rendszer elindulását. Hasonló helyzetet okozhat az is, ha valamelyik rendszerfile (NTLDR.EXE, NTOSKERNEL.EXE, Registry) megsérül. Az NT 4 környezetekben nehezen lehetett menet közben kikapcsolni a hibás eszközvezérlőket, és a rendszerállományok visszaállítása is körülményesnek bizonyult.
- *A dinamikus alkalmazás könyvtárak felülírása (A „DLL Hell" szindróma)*

  A korábbi 32 bites operációs rendszerek alatt az alkalmazások telepítője bármikor felülírhatta valamely korábban telepített program dinamikus könyvtárait az eredetitől eltérő verzióval. Ha a frissen telepített verzió korábbi volt, mint a már fennlévő program által igényelt, könnyen előfordulhatott, hogy e program elindíthatatlanná (vagy fagyásra hajlamossá) vált.

  Későbbi DLL-verzióval sem mindig tanácsos megajándékozni az alkalmazásokat, ez ugyanis szintén váratlan nehézségekhez vezethet.
- *Az eszközvezérlők és rendszerszolgáltatások által okozott „kék halál" (Blue Screen of Death)*

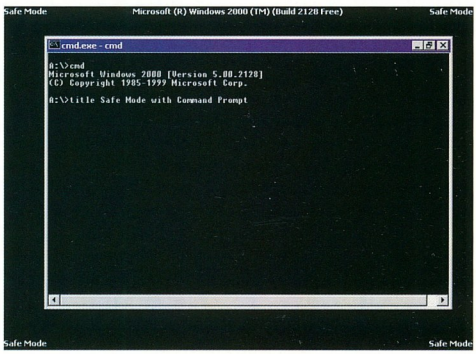
  A rettegett képernyő akkor bukkan fel, ha a rosszul megírt eszközvezérlő vagy rendszerszolgáltatás beleír valamelyik másik eszközvezérlő vagy a rendszer memóriaterületébe. A hibát ténylegesen kiváltó kód azonosítása éles rendszerekben gyakorlatilag lehetetlen.

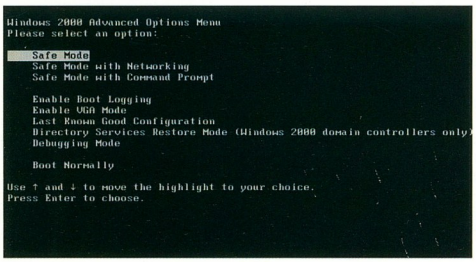
Lássuk hát, a fejlesztők mit tettek, hogy ritkábban, vagy jó esetben soha többé ne kelljen a fenti gondokkal birkóznunk!

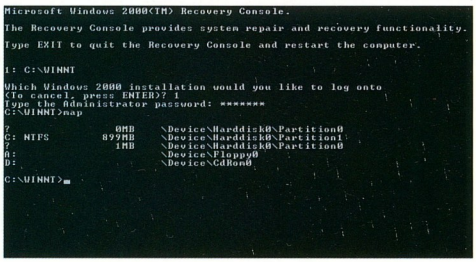
Safe Boot

A hibásan konfigurált operációs rendszer újraindíthatósága érdekében az NT 4 tartalmazott egy speciális indítási opciót, a *Last Known Good configuration*. Ha ezt választottuk, a legutolsó működőképes beállítások aktivizálásával a rendszer képes volt visszaállítani a pillanatnyi konfigurációt (*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*) valamelyik korábbi állapotba.

Sajnos, ez csak abban az esetben segített, ha a rendszer által ismert „legutóbbi működőképes" állapot valóban működőképes konfigurációt fedett. Amennyiben ez valamilyen okból szintén meghibásodott beállítás volt, az NT 4 csak a rendszer hivatalos visszaállító procedúráján (Emergency Repair Disk, Windows NT Setup) keresztül, vagy külső megoldások (www.sysinternals.com) segítségével volt helyreállítható.







Parancs	Funkció
ATTRIB	Megjeleníti a file-ok és a könyvtárak attribútumait
CD, CHDIR	Könyvtárat vált
CHKDSK	Ellenőrzi a megadott lemezt
CLS	Törli a képernyőt
COPY	File-t másol
DELETE, DEL	File-t töröl
DIR	Kilistázza a könyvtár tartalmát
DISKPART	Hozzáad vagy töröl partíciókat
ENABLE, DISABLE	Be- és kikapcsolja az eszközmeghajtókat és szervizeket
EXTRACT	Kibont adott állományt adott Cabinet (CAB) file-ból
FIXBOOT	Kijavítja a bootszektort
FIXMBR	Kijavítja a master boot rekordot
FORMAT	Lemezt formáz
LISTSVC	Kilistázza a szervizeket
LOGON	Bejelentkezik adott telepített rendszerbe
MAP	Megmutatja a meghajtó-betűjel-lemez összerendeléseket
MKDIR	Könyvtárat hoz létre
TYPE, MORE	Megmutatja egy file tartalmát
RMDIR	Töröl egy könyvtárat
REPAIR	Lecseréli adott telepített rendszer állományait a Windows 2000 CD-n található file-okra
RENAME, REN	Átnevez adott file-t vagy könyvtárat
SYSTEMROOT	Átvált a telepített rendszer gyökérkönyvtárába (pl.: \winnt)

A Recovery Console-on használható parancsok

E bonyodalmak elkerülésére a Windows 2000 tartalmazza a – Windows 9x operációs rendszerből már ismert – úgynevezett *Safe Boot* indítási lehetőséget, melynek segítségével a meghibásodott konfigurációt pillanatok alatt helyreállíthatjuk. Elég, ha rendszerindításkor az F8 billentyű megnyomásával a W2k-t csökkentett üzemmódban indítjuk el, majd inaktív állapotba helyezzük a gondot okozó szervizt vagy eszközt.

A Windows 9x-től eltérően azonban a W2k négyféle helyreállítási üzemmódban képes elindulni.

Az első lehetőség a *Standard Mode*, mely a működéshez szükséges minimális eszközvezérlőket és szolgáltatásokat engedélyezi.

Ezek listája megtalálható a registry *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal* kulcsa alatt.

Amennyiben a helyreállítási procedúra során a hálózatra is szükségünk van – például valamelyik eszközvezérlő-állomány frissítése céljából –, akkor választhatjuk a második, *Network Mode* nevű indítási opciót. Ez az alapvető hálózati vezérlőket és szolgáltatásokat *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network* is engedélyezi (sikeres bootra persze csak akkor számíthatunk, ha a lefagyáshoz vezető hiba nem éppen ezekben a rendszerösszetevőkben keresendő).

A grafikus kártyák rosszul megírt vezérlője a rendszer elindulásának további – meglehetősen gyakori – kerékkötője lehet, ennek „köszönhetően" az operációs rendszert még a minimális eszközvezérlőkkel sem tudjuk életre kelteni. Ekkor választhatjuk a harmadik indítási lehetőséget, a *Safe Mode with Command Prompt* opciót. Ezt kijelölve a *Standard Mode-dal* azonos rendszerszolgáltatások indulnak el azzal a kivétellel, hogy a grafikus felületen az Explorer helyett mindössze parancssori ablakot (CMD.EXE) kapunk. Ez alatt a grafikus adminisztrációs eszközök parancssoros verziójával tudjuk a „beteg" eszközvezérlőt kikapcsolni.

S végül, de nem utolsó sorban a Windows 2000 hálózatok idegrendszerét jelentő Active Directory szervizt futtató tartományvezérlők adatbázisainak meghibásodása esetén indulhatunk úgynevezett *DS-Repair Mode-ban* is. Fontos tudnunk azonban, hogy ez a mód csak akkor indítható el a tartományvezérlő szervereken, ha a rendszer standard és network módban használt szolgáltatásai egyébként működőképesek.

Gyakorlati tapasztalataink az mutatják, hogy a sérült vagy félrekonfigurált Windows 2000 szinte mindig elindítható Safe Mode-ban, így nyugodtan kicsit mélyebbre rejthetjük a telepítő CD-t és a javítólemezt.

Recovery Console

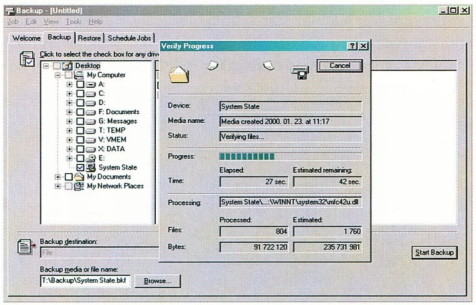
Az előzőekben említett Safe Mode indítási opciók rendkívül hasznosak bizonyos eszköz- és szervizspecifikus hibák elhárítására, ezzel azonban a rendszerünk stabilitását veszélyeztető jelenségek csak egy részét küszöböltük ki.

Hátra van még az az állapot, amikor a file-rendszer vírus- vagy hardverokokra visszavezethető meghibásodása esetén éppen a rendszerindító állományok (NTLDR.EXE, NTOSKERNEL.EXE, boot.ini, MBR, boot sector stb.) vagy a Safe Mode által igényelt standard eszközvezérlők és szervizek állományai sérülnek meg.

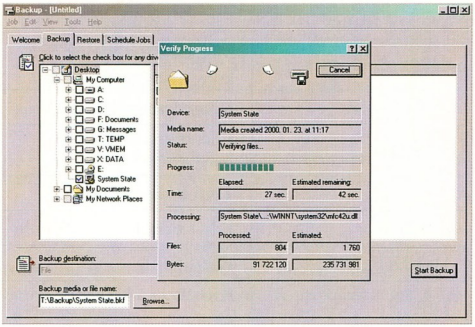
A hivatalos megoldás természetesen ilyenkor is az úgynevezett Emergency Repair Disk (ERD), vagy a telepítő készlet (floppy, CD) használata. A gond csak az, hogy a file-rendszer ilyen jellegű meghibásodásakor általában nincs szükség teljes rendszer-visszaállításra (rendszerállományok, registry stb.), sokszor elég, ha csak a sérült file-t vagy rendszerterületet frissítjük fel egészséges verzióval. Ez viszonylag könnyen megy akkor, ha a bootpartíció FAT-formátumú, mivel DOS-os indítólemezzel egyszerűen ellenőrizhetjük és javíthatjuk a merevlemez file-rendszerét. Nincs könnyű dolgunk, ellenben ha a rendszerpartíció NTFS file-rendszerrel lett formázva, mivel ezekhez a partíciókhoz csak külső gyártók által készített programokkal lehet hozzáférni.

A Windows 2000 *Recovery Console* szolgáltatása az ilyen gyors hibajavító beavatkozások elvégzésére született meg. Ennek segítségével akár az NTFS partíciókon tárolt rendszerállományainkat is felfrissíthetjük, illetve az NTFS file-rendszert ért sérüléseket is gond nélkül helyreállíthatjuk (FixMBR, FixBoot, Chkdsk). A szolgáltatást a telepítő médiákról indíthatjuk el, de a winnt32.exe/cmdcons paranccsal a kiszolgálóinkra vagy munkaállomásainkra is telepíthetjük, hogy mindig kéznél legyen.

A Recovery Console-lal kapcsolatban fontos tudnunk, hogy ez nem parancssorban elindított operációs rendszer, hanem az NT kernel egyedileg módosított futatható része, amely kizárólag adminisztrátorok számára teszi lehetővé a bejelentkezést, és számukra is csak a gyökér-, valamint a rendszerkönyvtárakhoz, illetve a cserélhető médiákhoz (floppy, CD) enged hozzáférést. A Recovery Console-on használható parancsokat az előző oldal *táblázata* foglalja össze.



Az NTBackup a kiszolgálókra telepített összes kritikus rendszerösszetevő adatait képes menteni



DLL Cache

NTBackup

A rendszerünk épségét veszélyeztető helyzetek elemzésében eljutottunk a lehető legsúlyosabb állapotig: az előző két eset kombinációjaként jelentkező teljes rendszerösszeomláshoz. Bizony, ilyenkor nem segít más, mint a megfelelő rendszerességgel elkészített biztonsági mentés. Szerencsére a Windows 2000 ezen a területen is tartalmaz rendkívül hasznos újdonságokat. A nem csupán új külsővel, de új szolgáltatásokkal is megjelenő NTBackup program is ezek közé tartozik.

Egyik ilyen újdonság, hogy az ERD-lemez készítése közvetlenül ebből az alkalmazásból indítható el.

Fontosabb azonban az, hogy az NTBackup a standard adatmentési lehetőségek mellett a kiszolgálókra telepített összes kritikus rendszerösszetevő adatait is képes lementeni.

Ezek közé a következő szervizek adatbázisai tartoznak:

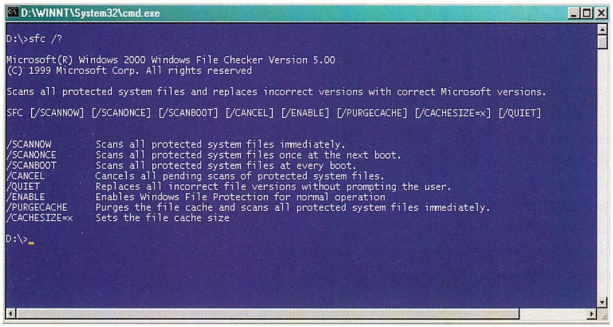
- Registry;
- COM+;
- Tanúsítványkiadó Hivatal (Certificate Service);
- Active Directory DIT;
- File Replication;
- Cluster Server quorum log.

●

A Safe Boot, a Recovery Console és az NTBackup új szolgáltatásaival röviden áttekintettük a Windows 2000 elindulását megakadályozó jelenségeket és a kiküszöbölésükre készült eszközöket. Következő állomásunk a már működő rendszer egységét veszélyeztető helyzetek, valamint az elkerülésüket célzó W2k-s technológiák számba vétele.

Windows File Protection

A Windows NT-s rendszerekben a gyakran „DLL Pokolként" (DLL Hell) emlegetett jelenség sok gondot okozott. Mint már szó volt róla, adott alkalmazás (sőt, maga a rendszer is) instabillá válhat, ha valamelyik másik program telepítője felülír-



A WFP szerviz parancssorból is aktivizálható

ja az általa használt dinamikus könyvtárat névleg azonos, de más verziójú állománnyal. A következmény: az eredeti dinamikus könyvtár által adott függvények elérhetetlenné válnak, vagy működésük némiképp megváltozik.

A W2k Windows File Protection (WFP) szervize e jelenség kiküszöbölésére született meg.

A WFP egyfajta file-rendszer őrszemként folyamatosan ellenőrzi a rendszerkönyvtár *(%systemroot%)* alatti közel 3000 kritikus állományt, melyek között a DLL-ek mellett számos programot (EXE), ActiveX-vezérlőt (OCX), eszközvezérlőt (DRV, SYS), valamint rendszerfontot, telepítő (INF) és digitális aláírás katalógust (CAT) is találhatunk.

Amennyiben valamelyik alkalmazás megpróbálja átírni bármelyik kritikus állományt, a file-rendszer az eseménykezelő mechanizmusain keresztül (NTFS Change Journal) értesíti a WFP szervizt, amely visszaállítja a file-t az erre a célra kijelölt védett könyvtárból (DLL Cache). A Cache akár a központi megosztott meghajtón is elhelyezkedhet.

A WFP szerviz egyébként nemcsak a rendszer által, hanem parancssorból is aktivizálható.

A WFP az alkalmazások telepítése és futtatása szempontjából rendkívül hasznos szolgáltatás bevezetésével kapcsolatban azonban jogosan merül fel a kérdés: mi történik, ha valaki a DLL Cache könyvtár tartalmát írja át?

Nos, a valóságban ez közel sem olyan egyszerű művelet. A DLL Cache-t ugyanis a WFP a többi rendszerkönyvtárhoz hasonló módon védi, mégpedig azzal a hozzáadott funkcióval, hogy a DLL Cache-be csak hiteles digitális aláírással bíró állományok kerülhetnek be, ezek forrásai pedig csak a következők egyike lehet: a Windows Update, a Service Packek és a Hotfix csomagok.

Service Pack slipstreaming

Az NT-ben állandó gondot jelentett, hogy ha valamilyen új szolgáltatást vagy a rendszerben is mutató alkalmazást telepítettünk, utána mindig újra le kellett futtatni az aktuális Service Packet, hogy régebbi rendszerfile-ok ne keveredhessenek a rendszerbe.

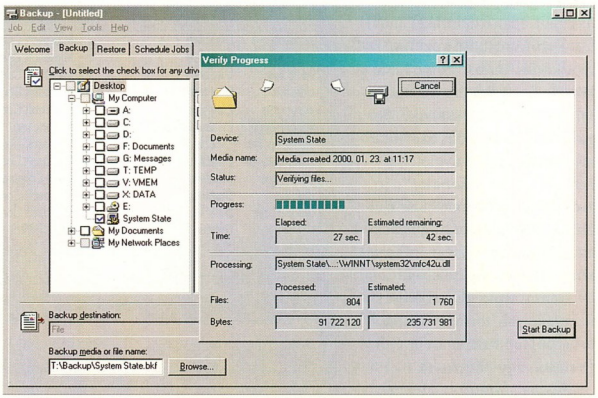
A Windows 2000 erre is ad gyógyírt a Service Pack slipstreamingnek keresztelt megoldással. E szolgáltatás folyamatosan figyeli a rendszerfile-okat, és ha változást észlel, automatikusan újratelepíti az érintett állományokat az aktuális szervizcsomagból. Csakúgy, mint a DLL Cache-t, a szervizcsomagot is tehetjük központilag megosztott meghajtóra.

Driver Signing

Korábban már említettem, hogy valamely operációs rendszer előre nem látható meghibásodásainak elsődleges forrása az alacsony színvonalon megírt eszközvezérlőkben keresendő.

A Microsoft az NT 4 megjelenése óta kiadja, és folyamatosan frissíti azt a kompatibilitási listát (HCL), amelyben felsorolja a hivatalos tesztlaborok által bevizsgált és minősített hardvereszközöket.

Sajnos, a tapasztalataink azt mutatják, hogy sokan még az úgynevezett üzletileg kritikus (Mission Critical) alkalmazásokat sem a bevizsgált hardverösszetevőkön, hanem ellenőrizetlen eszközvezérlőkkel futtatják. Ennek egyik oka az, hogy a rendszeradminisztrátorok az eszközök telepítésének pillanatában nem ellenőrizhetik, hogy a telepíteni kívánt eszköz adott

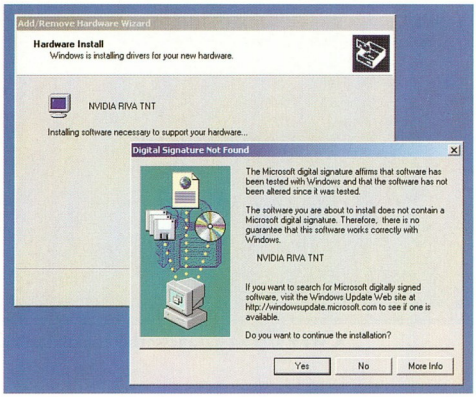


A Driver Signing technológia bekapcsolásával a rendszerbe csak megfelelő digitális aláírással hitelesített eszközvezérlők települhetnek

eszközvezérlője és annak verziószáma HCL kompatibilis-e vagy sem.

A Windows 2000-ben a Driver Signing technológia az ilyen esetek elkerülésére született meg. Bekapcsolásával a rendszeradminisztrátorok előírhatják, hogy a rendszerbe csak a Microsoft által minősített és a megfelelő digitális aláírással hitelesített eszközvezérlők települhetnek

A Driver Signing által alkalmazott védelmi rendszer nem új keletű. A W2k ebben ugyanazt a hitelesítési mechanizmust használja, mint amelyiket az Internet Explorer az ActiveX összetevők letöltése során alkalmaz (Authenticode). A Driver Signing további előnye, hogy az Active Directory által nyújtott központi rendszermenedzsment-technológiák (Group Policy Objects) segítségével akár a hálózat összes szervere és munkaállomása számára előírhatjuk, hogy azokra csak digitális aláírással bíró eszközök települhetnek.



●

Végezetül térjünk át a rendszer teljes összeomlását előidéző, a hírhedt, s sokak által „Kék Halál" néven ismert jelenség ismertetésére.

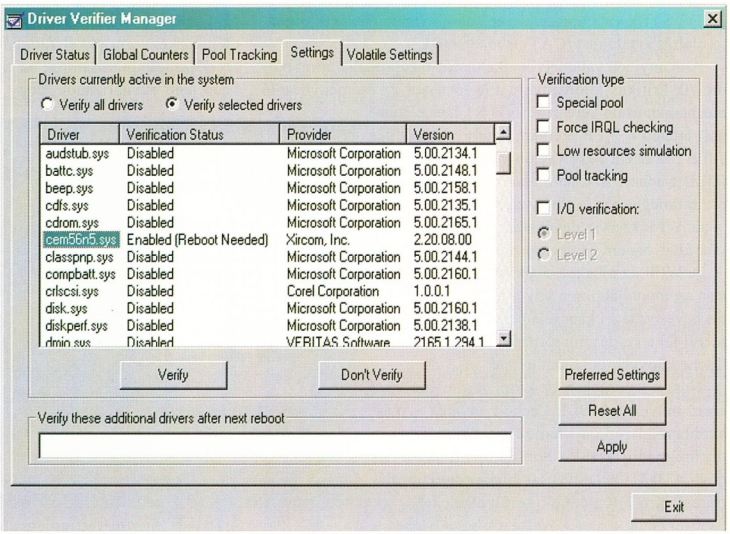
A W2k fejlesztői kiemelt figyelmet szenteltek annak, hogy ez a váratlan rendszerleállás a lehető legkevesebb esetben következzen be. De mielőtt közelebbről is megvizsgálnám az ezzel kapcsolatos újdonságokat, tekintsük át röviden, hogy valójában mi is történik az NT kulisszái mögött a „Blue Screen" beálltakor.

A kék halál forrása a kernelszinten futó eszközvezérlők hibás memóriakezelése. Az eszközvezérlők, mint minden program, a futásuk során használt adatstruktúrákat mutatókon keresztül kezelik, s rendkívül fontos, hogy futás közben azok mindig a megfelelő helyre mutassanak. Ha valamelyik eszközvezérlő a memóriakezelő műveletei során „elveszti a fonalat", jó eséllyel a vele azonos szinten működő rendszer- vagy más eszközvezérlő adat- vagy kódterületébe fog beleírni.

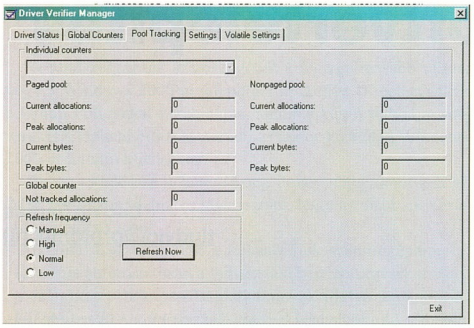
A mutatókezelési hibák leggyakoribb forrása valamelyik puffer túlírása (buffer overrun vagy underrun).

Kósza mutatókat természetesen az úgynevezett *User Mode-ban* futó hétköznapi alkalmazások is tudnak produkálni – néha túl sokszor is. Ezek során azonban mindössze a „General Protection Fault" az eredmény, ugyanis a hibát a kernel privilegizált módban futó kivételkezelő mechanizmusai lekezelik anélkül, hogy az írási kísérlet kárt okozna más rendszer- vagy alkalmazás-folyamatokban.

A fentiek ismeretében most már világos, mit jelent a kék halál: az operációs rendszer kivételkezelője által észlelt hibás memóriakezelő műveletet, amely során a rendszer a további



A rendszer stabilitását veszélyeztető helyzetekről eseménynapló bejegyzés készül



A központi memóriafoglalásokat is nyomon követhetjük

esetleges súlyosabb meghibásodások – file-rendszer, registry – elkerülése céljából leáll (Bug Check).

Ahhoz, hogy ez minél kevesebbszer fordulhasson elő, a W2k fejlesztői két rendkívül hasznos kernelszintű védelmi mechanizmust fejlesztettek ki.

Write-Protected System Code

A Blue Screen elleni védekezés első vonalában olyan szolgáltatást találunk, amely a privilegizált módban futó programok kódterületeit védi. A W2k memóriakezelője a registry *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\MemoryManagerEnforceWriteProtection* kulcsában beállítottak szerint a kernel és az összes aktív eszközvezérlő memóriaterületét képes átállítani csak olvasható módba.

A csak olvasható memóriát a lapvédelmi rendszer már hatékonyan tudja óvni. Az eltévedt kernelmodulok próbálkozásairól a továbbiakban azonnal bejegyzés készül a rendszer eseménynaplójában, ennek segítségével az operációs rendszer mélyén garázdálkodó folyamat egyértelműen azonosíthatóvá válik.

Driver Verifier

Az is a hírhedt képernyő felbukkanásához vezethet, ha valamelyik félresikerült memóriaallokációs művelet a kernel betölthető moduljainak (Loadable Modules) adatterületét veszélyezteti. Ez a hiba is rendkívül nehezen azonosítható, mivel a rendszerszinten futó külső kódrészletek adatai gyakorlatilag egyenrangúak a kernel moduljaival. Következésképpen adott rendszerszintű memóriakezelő művelet kiszolgálásakor az operációs rendszer nehezen tudja eldönteni, hogy adott belső hívás tulajdonképpen értelmes vagy értelmetlen adatterület-módosító feladatot kér-e. A virtuális memóriakezelő ezért gáláns módon megbízik minden privilegizált szinten futó folyamatban, s kiszolgál bármilyen igényt, legyen az akár valamilyen másik kernelmodul vagy a rendszer saját adatterületeire mutató hívás.

A bajokat tovább fokozza, hogy az ilyen esetek következményei nem azonnal mutatják meg magukat. A végső utasítás, mely a rendszerösszeomlást okozza valójában már csak egyik következménye a korábbi hibás memóriakezelő műveletnek.

Mivel a fenti jelenség kiküszöbölésével a rendszerösszeomlások igen nagy hányada elkerülhető lenne, a Microsoft fejlesztői fokozott figyelmet szenteltek egy olyan rendszerösszetevő kifejlesztésének, amelynek a segítségével a hibás belső memóriaművelet már bekövetkezése pillanatában azonosítható.

A megoldást pedig a Driver Verifier nevű kernelmodul és a hozzá kapcsolódó grafikus alkalmazás jelenti, mely minden bizonnyal a Windows 2000 megbízhatóságának egyik legfontosabb építőköve. Működését tekintve a rendszerösszetevők védelméhez hasonlóan a Driver Verifier a kernel betölthető moduljainak adatterületére mutató memóriaallokációs műveleteket felügyeli.

Segítségével választható módon vagy az összes privilegizált szinten futó, vagy csak az általunk gyanúsnak ítélt rendszerösszetevőkre vonatkozóan előírhatjuk, hogy azok csak a Driver Verifieren keresztül hajthassanak végre memóriaműveleteket.

A továbbiakban ezekről a hívásokról statisztika, a rendszer stabilitását veszélyeztető helyzetekről pedig eseménynapló bejegyzés készül.

A Driver Verifier amellett, hogy naplóz, még egyéb érdekességekre is képes. Segítségével nemcsak észlelhetjük, hanem akár elő is idézhetjük a rendszerünk integritását veszélyeztető helyzeteket.

Szimulálhatjuk például a memória elfogyását (*Low resources simulation*), ez ugyanis a nem megfelelő hibakezelésű eszközvezérlőket könnyedén térdre kényszerítheti.

Emellett figyelemmel kísérhetjük a központi memóriafoglalásokat (*Pool Tracking*), vagy az eszközvezérlők viselkedését a különböző megszakításszintek (IRQL) váltásakor.

A Microsoft is alaposan kihasználta e szolgáltatást fejlesztés közben, ez nagymértékben hozzájárult a Windows 2000 használata során észlelt általános stabilitásérzethez. A Driver Verifier azonban nemcsak a fejlesztők, hanem a rendszeradminisztrátorok egyik fontos diagnosztikai eszköze is.

Szép új évezred

Mint a fentiekből kiderült, a Windows 2000 a legtöbb, a rendszer stabilitását veszélyeztető, illetve újraindítását lehetetlenné tevő helyzetet segít kiküszöbölni. Ezt részben az új Safe Mode-dal, részben a DLL-ek felülírásának megakadályozásával, részben pedig a privilegizált szinten futó eszközvezérlők memóriaműveleteinek jobb védelmével éri el.

Összegzésként elmondhatjuk, hogy az újításoknak köszönhetően a Windows 2000 alapvetően megbízhatóbb futtatási környezetet teremt mind a népszerű 32-bites ügyféloldali alkalmazásoknak, mind pedig a Windows 2000 kiszolgálócsalád köré épülő következő generációs platformszolgáltatások számára.

Automatikus szoftvertelepítés és karbantartás

Ludvig Tamás
tludvig@protomix.hu

A Windows 2000 automatikus szoftvertelepítési képessége lehetővé teszi a rendszergazdák számára a vállalat szoftvereinek – beleértve az alkalmazásokat, a javító csomagokat és az operációs rendszer upgrade-jét – rugalmas és kényelmes távoli menedzselését.

Nehéz olyan beruházást találni, melyben a lehető legkisebb költség nem szerepel a fontossági sorrend élén. A számítógépes infrastruktúra sem kivétel, a vállalatok szeretnék, ha a masinák a lehető legolcsóbban oldanák meg minden gondjukat. A Windows 2000 kifejlesztésekor a Microsoft több lépést is tett a TCO (Total Cost of Ownership) csökkentésére, ezek között az automatikus szoftvertelepítés és karbantartás fontos szerepet játszik.

Az Active Directory, a Group Policy, a Windows Installer technológia és az Add/Remove Programs együttese jelentősen növeli a szoftverek elérhetőségét, és minimalizálja az adminisztrációs teendőket.

A Windows telepítési technológiája

A szoftvertelepítés és karbantartás a Windows 2000-ben a Windows Installer szerviz segítségével történik, ami megváltás a legtöbb felhasználó számára.

Régóta vágyott mindenki olyan egységes telepítési módszerre, amely automatikusan képes a nagyvállalati rendszerekben leggyakrabban előforduló feladatokat elvégezni, valamint ezerféle többé-kevésbé házi barkácsolású telepítőnél konzisztensebben és robosztusabban működik.

A Windows Installer szerviz a következő összetevőket tartalmazza:

– rezidens telepítő szerviz,
– standard formátum a komponens-menedzsmenthez,
– menedzsment API az alkalmazások és eszközök számára.

A Windows Installer technológia új file-formátumot használ, melyet Windows Installer csomagnak vagy röviden .MSI file-nak hívnak. Az .MSI file-ok a korábban alkalmazott SETUP.EXE file-okat váltják fel, és sokkal magasabb szintű, kifinomultabb szoftvertelepítést, valamint karbantartást tesznek lehetővé. A technológia legnagyobb előnyei a következők:

- Inkrementális telepítés: az Office 2000 jó példa erre, ennek bizonyos funkciói csak akkor települnek, amikor először használjuk őket (pl.: a varázslók). Ez a megoldás csökkenti a telepített alkalmazás helyigényét.
- Önjavító alkalmazások: ha valamelyik kritikus file hiányzik vagy sérült, akkor az alkalmazás automatikusan letölti a szükséges file-t a hálózati share-ről, ahonnan az eredeti telepítés is történt. Mindez a háttérben zajlik, nincs szükség a felhasználó beavatkozására.
- Az alkalmazások úgy távolíthatók el a munkaállomásokról, hogy nem hagynak maguk után „szemetet", illetve nem távolítanak el olyan file-okat, amelyek más alkalmazások működéséhez is szükségesek. Mindezek az előnyök nemcsak a Windows 2000-es környezetben használhatók ki, hanem a Windows NT 4.0, a Windows 95 és a Windows 98 operációs rendszerek alatt is élvezhetjük őket, ha telepítjük a Windows Installer megfelelő változatát.

A vájtfülűbbeknek feltűnhetett, hogy ez a technológia nem teljesen forradalmi, hasonló elven működő alkalmazástelepítést már az SMS (System Management Server) is tudott a munkaállomásokon futó PCM szerviz segítségével. Ezzel a módszerrel felhasználói beavatkozás nélkül lehetett alkalmazásokat telepíteni, valamint az operációs rendszer beállításait módosítani.

Szoftvertelepítési és karbantartási technológia

A rendszergazdák szemszögéből a legizgalmasabb újítás, hogy a Windows 2000 új telepítőjét az Active Directoryval és a Group Policykkal kombinálva, automatikusan tudunk szoftvereket telepíteni és karbantartani a (sajnos kizárólag Windows 2000-et futtató) klienseken.

Ehhez mindössze néhány Group Policy objektumot kell az .MSI file-hoz rendelni, és kiválasztani, hogy az alábbiak közül mit szeretnénk tenni:

- Alkalmazások telepítése a felhasználók számítógépein. Ez történhet automatikusan a felhasználó bejelentkezésekor vagy a számítógép bekapcsolása alkalmával, illetve manuálisan. Utóbbi esetben a felhasználó csak akkor telepíti az alkalmazást, amikor szüksége van rá.
- Az alkalmazás korábbi verziójának upgrade-je, valamint javítócsomagok automatikus telepítése.
- Alkalmazások automatikus eltávolítása a számítógépekről.

Publish vagy assign

A rendszergazdák alapvetően kétféle szoftver-disztribúció közül választhatnak:

- **Publish**: a rendszergazda publikálhatja azokat az alkalmazásokat, amelyekre a dolgozóknak esetleg szüksége lehet, a felhasználó eldöntheti, hogy telepíti-e valamelyiket vagy sem.
- **Assign**: a rendszergazda hozzárendelheti az egyes felhasználókhoz azokat az alkalmazásokat, amelyekre a munkavégzéshez feltétlenül szükségük van. Ha ezt a módszert választjuk, akkor az alkalmazás ikonja automatikusan megjelenik a felhasználó Start menüjében.

Mint az a táblázatból is kiderül, assign esetén az alkalmazást nemcsak a felhasználóhoz, hanem a számítógéphez is rendelhetjük. Ebben az esetben az alkalmazás mindig elérhető az adott munkaállomáson függetlenül attól, hogy éppen ki jelentkezik be. Ez a megoldás nagyon hasznos lehet például Office 2000 tanfolyamon az osztályteremben, mikor minden tanuló használja a programcsomagot, de a diákok nem mindig ugyanazon a helyen ülnek, ráadásul rendszeresen cserélődnek.

Telepítő file-ok elkészítése

Adminisztrátorként nem az interaktív varázslók, hanem a kész telepítési konfigurációkat tároló Windows Installer file-ok a szoftvertelepítési és karbantartási technológia legérdekesebb részei. Ez persze azt is jelenti, hogy mindenek előtt szükségünk van valamilyen MSI állományra.

De honnan is származik ez?

- Beszerezzük a szoftvergyártótól.
- Elkészítjük a megfelelő szoftver segítségével.
- Szöveges .ZAP file-ként megkomponáljuk.

MSI file-ok készítése

A legkényelmesebb (és leg-TCO-barátabb) eset, ha olyan alkalmazást szeretnénk telepíteni, amely gyárilag támogatja a Windows Installer technológiát. Pillanatnyilag ez a szoftverek kisebbik része, élükön a Microsoft Office 2000-rel. Szerencsére már több olyan eszköz létezik, amellyel a gyártók, vagy akár mi magunk is elkészíthetjük a szükséges MSI file-okat, például:

- InstallShield for Windows Installer (InstallShield Software Corporation – www.installshield.com),

	Publish	Assign (felhasználó)	Assign (számítógép)
Miután az adminisztrátor elvégezte a szükséges beállításokat, az alkalmazás települ.	A következő bejelentkezés után.	A következő bejelentkezés után.	A számítógép újraindítása után.
A felhasználó tipikusan a következő helyről tudja telepíteni a programot.	Az Add/Remove Programsból a Control Panelen.	Az Add/Remove Programsból a Control Panelen, a Start menüből, ill. a munkaasztalról shortcut segítségével.	Az alkalmazás automatikusan települ, a felhasználónak nem kell tennie semmit.
Ha az alkalmazás nincs telepítve, és a felhasználó megnyitja az alkalmazást, akkor az automatikusan települ?	Igen.	Igen.	Az alkalmazás automatikusan települ, a felhasználónak nem kell tennie semmit.
A felhasználó el tudja távolítani az alkalmazást az Add/Remove Programs használatával?	Igen és a későbbiekben ismét telepítheti is az Add/Remove Programsból.	Igen, de a következő bejelentkezéskor az alkalmazás ismét települ.	Nem, csak a lokális Adminisztrátor tudja eltávolítani az alkalmazást. A felhasználó csak javítást futtathat az alkalmazásokon.
Támogatott file-típusok	Windows Installer csomagok (.msi filel-ok), .zap file-ok.	Windows Installer csomagok (.msi file-ok).	Windows Installer csomagok (.msi file-ok).

A publish és az assign legfontosabb tulajdonságai

- Wise for Windows Installer (WISE Solutions Inc.– www.wisesolutions.com),
- WinInstall LE (Seagate Software – www.seagatesofware.com/winstall).

A WinInstall LE megtalálható a Windows 2000 Server CD-n is.

Az eszközök birtokában remélhetőleg a gyártók is mihamarabb Windows Installer-baráttá fogják tenni alkalmazásaikat megkímélve minket a házi bütyköléstől.

.ZAP file-ok készítése

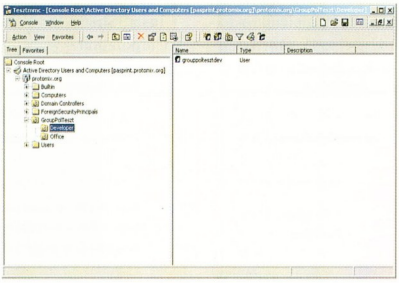
Ha az .MSI file beszerzése vagy összebarkácsolása reménytelen, akkor .ZAP file elkészítésével is rábírhatjuk az Installert, hogy telepítse alkalmazásunkat (a hagyományos setup.exe használatával). A legfőbb korlátozás, hogy a programok így csak publikálhatók a felhasználók felé, valamint az alábbi .MSI által nyújtott előnyöket is elveszítjük:

- automatikus telepítés a program első használata alkalmával,
- emelt szintű jogosultságok alkalmazása a szoftvertelepítés során,
- az alkalmazások egyes szolgáltatásainak automatikus telepítése az első használatkor,
- a telepített alkalmazás módosítása, illetve javítása vagy sikertelen telepítés esetén eltávolítása.

A .ZAP file-ok szöveges file-ok (hasonlók az .INI file-okhoz), ezekben le kell írni, hogyan kell telepíteni az alkalmazást, valamint fel kell sorolni annak legfontosabb tulajdonságait (név, verzió, nyelv). A kész .ZAP-ot általában célszerű ugyanoda tenni, ahol a hozzá tartozó telepítő program van.

Telepítő file-ok módosítása .MST file-okkal

Hasznos újítás, hogy nem kell megelégednünk az .MSI file-ba beledrótozott alapértelmezett telepítéssel, hanem többféle saját konfigurációt is létrehozhatunk. Az Office 2000 példájára visszatérve, megadhatjuk, hogy adott felhasználó csoport számára csak az Excel települjön automatikusan, a csomag többi része ne.



Személyre szabott Tesztmmc konzol

A gyakorlatban először az egyedi konfigurációt .MST telepítő file-ban kell összeállítani. Ha ez kész, létre kell hozni az egyes felhasználói csoportoknak megfelelő szervezeti egységeket (Organizational Unit – a továbbiakban OU), majd különkülön Group Policy objektumokat (GPO) kell definiálni, amelyekben a megfelelő módosító file-t (.MST) adjuk meg az eredeti .MSI file-hoz (pl. *Group Policy/User Configuration/Software Installation/Package Properties/Modifications*).

A szoftver disztribúció kialakításának folyamata

Ha az alkalmazások telepítéséhez szükséges file-ok már megvannak, akkor nincs más hátra, mint elérhetővé kell tenni azokat a hálózaton, és a Group Policyban végre kell hajtani a szükséges beállításokat.

Szoftver-disztribúciós pont létrehozása

A menedzselendő alkalmazások file-jainak (.MSI és .ZAP file-ok, valamint a szoftverek egyéb file-jai) elérhetőnek kell lenniük a hálózaton. A rendszergazdának hálózati share-t kell létrehoznia a megfelelő könyvtárszerkezettel, és a telepítéshez szükséges file-okat be kell másolnia a megfelelő könyvtárakba. Ne feledkezzünk meg róla, hogy a célfelhasználóknak legalább olvasási jogot kell adni a share-re (Everyone = read, Administrators = Full Control, Change, Read).

Beállítások a Group Policyban

Az rendszergazdák a Group Policy segítségével valósíthatják meg az alkalmazások automatikus telepítését.

A *Management Console-ban* (MMC) az *Active Directory Users and Computers snap-in* eszközzel lehet létrehozni az OU-okat, és az egyes szervezeti egységekhez egy vagy több GPO-t lehet rendelni. A GPO szerkesztésével lehet beállítani, hogy számítógéphez vagy felhasználóhoz rendeljük-e az adott alkalmazást, illetve a szoftver-disztribúció típusa publish vagy assign legyen-e.

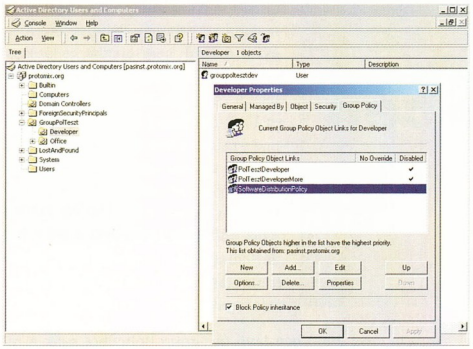
Létrehozhatunk .MSC file-okat is a felügyeletünk alatt álló OU-ok egyszerűbb elérésére.

Delegált jogok alkalmazása esetén (pl.: adott OU adminisztrációját egy jól meghatározott személy végzi) mindenképpen célszerű elkészíteni ilyen .MSC file-t. A későbbiekben ezt az MMC-ben már csak meg kell nyitni.

Alkalmazások eltávolítása

A Windows 2000 a régi (de már MSI file-lal és Group Policy segítségével telepített), használaton kívüli alkalmazások eltávolításában is segít kétféle választást kínálva:

- Kényszerített eltávolítás: az alkalmazás automatikusan törlődik a számítógépről az újraindítás után (Computer Policy), illetve a felhasználó következő bejelentkezésekor (User Policy).
- Nem kötelező eltávolítás: az alkalmazás nem törlődik automatikusan a számítógépekről, de új felhasználók már nem telepíthetik.



Software Distribution Policy GPO hozzárendelése a Developer OU-hoz

Hasznos tippek

Az alábbiakban néhány megszívlelendő tanácsot szeretnék adni azok számára, akiket már erősen foglalkoztat a gondolat, hogy alkalmazásaik telepítését Windows 2000-es alapokra helyezzék.

Az első és legfontosabb teendő az, hogy felmérjük, milyen programokra van egyáltalán szükségünk. Sajnos általánosan jellemző, hogy a munkaállomásokon sok olyan alkalmazás van, amelyekre semmi szükség a mindennapi feladatok ellátása során, csak foglalják a helyet, és néha adminisztrációs galibákat okoznak.

A szükségesnek ítélt alkalmazásokat soroljuk csoportokba aszerint, hogy melyik telepítési mód a legelőnyösebb számunkra:

- A számítógépekhez rendeljük hozzá azokat az alkalmazásokat, amelyeket mindenki használ, így bárki bármelyik gép elé ül le, nem kell kivárnia a telepítést. Ezzel a megoldással a hálózati forgalmat is csökkenthetjük.
- Rendezzük csoportokba a felhasználókat az általuk használt alkalmazások szerint, készítsük el az OU-kat az egyes felhasználói csoportoknak, és rendeljünk hozzájuk GPO-kat.
- Vizsgáljuk meg, hogy az alkalmazások .MSI file-jai beszerezhetők-e, vagy el tudjuk-e készíteni ezeket, mert egyébként csak publikálni tudjuk az alkalmazást (.ZAP file készítésével).
- Ha nem tudjuk eldönteni, hogy számítógéphez vagy felhasználóhoz rendeljünk-e valamilyen alkalmazást, akkor inkább az utóbbit válasszuk, mert így csak akkor foglal helyet a helyi meghajtókon, ha ténylegesen használják (rákattintottak az ikonjára).

Az új telepítő file-okat (.MSI vagy .ZAP) elkészítésük után alaposan tesztelni kell, még mielőtt a munkaállomásokon installálnánk őket. Ehhez célszerű külön OU-okat készíteni, ezekbe új felhasználókat létrehozni, és néhány munkaállomást idemozgatni. Ezekhez rendeljük hozzá az alkalmazásokat a Group Policyn keresztül. Ha a telepítő file-ok jól működnek, akkor az összes munkaállomásra kiterjeszthetjük a Group Policyt.

Érdemes a Windows 2000 Server elosztott file-rendszer (Distributed File System) szolgáltatását is hadrendbe állítani a szoftver-disztribúció segítésére.

Ha valamely alkalmazást több változatban is szeretnénk telepíteni (pl.: Office 2000), akkor figyeljünk arra, hogy az .MST file-okat is akkor állítsuk be, amikor a telepítő file-t hozzárendeljük a felhasználóhoz vagy a számítógéphez.

Készítsünk kategóriákat az alkalmazásoknak (pl.: MS Office). Ez különösen akkor kedvező, ha sok van belőlük, és az *Add/Removes Programsban* már áttekinthetetlenül hosszú lista jelenik meg.

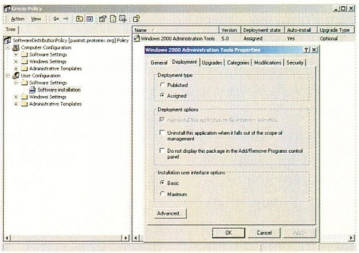
Az alkalmazások telepítése által generált hálózati forgalom és a programok lokális helyigénye között meg kell találnunk a helyes középutat. Ha ugyanis minden alkalmazást számítógéphez rendelnénk, akkor nagy méretű háttértárra lenne szükségünk, ha viszont mindent a felhasználókhoz, akkor a hálózati forgalom lehetne kritikus.

A munkaállomások alapösszetevőinek telepítését (számítógéphez rendelt programok) célszerű különálló, nagy sebességű hálózaton végezni.

Összegzés

A Windows 2000-ben alkalmazott szoftvertelepítési és karbantartási technológia segít a TCO csökkentésében az alkalmazások távoli menedzselhetőségének megteremtésével. Nagy előnyt jelent továbbá, hogy az egész folyamat egyetlen központi helyről menedzselhető, nem kell egyébként bejárni az összes munkaállomást, ha módosításokat kell végrehajtani a szoftver-konfigurációban.

A gyakorlati tapasztalataink azt mutatják, hogy a Microsoft Office 2000 és a Windows 2000 Administration Tools eredeti .MSI file-jaival, illetve az általunk készített .ZAP file-okkal a szoftvertelepítés minden szolgáltatása hibátlanul működik. Az .MSI file-ok készítésével viszont nehézségeink voltak, a korábban említettek közül a Segate Software WinInstall LE alkalmazását tudtuk legjobban használni. Reményeink szerint a jövőben az egyes szoftvergyártók automatikusan elkészítik majd a termékeik .MSI file-jait is.



Adminisztratív eszközök hozzárendelése felhasználói csoporthoz a Group Policyban

Group Policy a Windows 2000-ben

Holló Attila
ahollo@protomix.hu

Az Active Directoryval együtt megjelent Group Policy nagymértékben leegyszerűsíti a számítógépek és felhasználók menedzsmentjét a nagyobb hálózatokban. Ezáltal az adminisztrátorok munkája hatékonyabbá válik, az informatikai költségek pedig csökkennek.

A Windows 2000-ben lévő Group Policyval (csoportos házirend, a továbbiakban GP) központilag szabályozhatjuk a hálózatban megtalálható – mind a munkaállomás, mind pedig a szerver – számítógépek és felhasználóik „környezetét".

A módszer az NT-ben alkalmazott System Policynak erősen továbbfejlesztett változata. A Windows 2000 Group Policyban lehetőség van **registry** és **security** beállításokra, de a policy segítségével **szoftvert is telepíthetünk** (lásd *Automatikus szoftvertelepítés és karbantartás* című cikkünket).

startup, **shutdown**, **logon** és **logoff** scripteket állíthatunk be, valamint ennek közreműködésével a felhasználó rendszerszintű, a profile-ban megtalálható könyvtárai átirányíthatók.

A házirend felhasználásával úgy is be lehet állítani, illetve korlátozni a felhasználó környezetét (Desktop, Start menü, alkalmazások stb.), valamint a számítógépeket (Quota, Offline files stb.), hogy minél kevesebb lehetőség legyen az általa használt operációs rendszer és az alkalmazások „elkonfigurálására", azaz a környezet véletlen vagy szándékos átállítására.

Újdonságok

A Windows 2000-ben lévő új Group Policyból csak a registry beállítás volt az NT-ben is fellelhető. A többi új összetevő főleg a központi adminisztráció támogatására készült. A GP nagymértékben megkönnyíti ugyan ezt a feladatot, de a beállításához néhány esetben pilótavizsga szükséges.

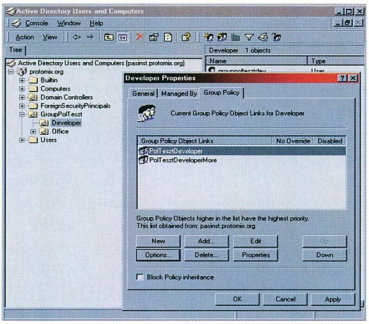
Az NT 4-ben megtalálható Policy Editorhoz képest, melyben a policy file módosítása körülményes volt, az új környezetben a Microsoft Management Console-on (továbbiakban MMC) keresztül, központilag módosíthatjuk a házirendet. Szintén jelentős különbség, hogy a régi domaines policyhoz képest, itt a site-hoz, a domainhez és a szervezeti egységhez (Organizational Unit, OU) is rendelhetünk policyt, így ki tudjuk használni az Active Directory (továbbiakban AD) által kínált lehetőségeket.

További változás, hogy a registry beállítások nem írják felül a registry kulcsokat, hanem az erre elkülönített helyre írnak. Gyakori hibalehetőséget lehet elkerülni e módszer bevezetésével. Ennek akkor van jelentősége, ha a felhasználó átkerül valamilyen másik policy-csoportba, vagy csak egyszerűen valamelyik régebben beállított kulcsot „nem konfigurált" állapotba helyezünk. Az NT-s policyban ebben az esetben a korábbi beállítások megmaradtak, és ezen rendszerint csak úgy lehetett segíteni, ha a felhasználó registry file-ját (NTUSER.DAT) letöröltük.

A Windows 2000-ben megtalálható jogosultsági rendszert – minden objektumhoz, containerhez hozzáférési jogot lehet megadni – a házirendre is kiterjesztették, azaz pontosan szabályozható, hogy ki milyen jogosultsággal férhet hozzá adott szervezeti egységhez vagy Group Policy Objecthez (csoportos házirend objektum, továbbiakban GPO).

Lehetőség nyílik a biztonsági beállítások (Security Settings) kezelésére is, elsősorban a számítógépek védelmére. Ennek során a munkaállomás minden olyan objektumára hozzáférési jogokat lehet beállítani, ahol ennek értelme van (például registry, file-ok, könyvtárak, audit, Kerberos stb.). Például azt is megtehetjük, hogy a GP-vel telepített szoftver file-jaihoz automatikusan NTFS jogokat is beállítunk, vagy szabályozzuk a program által használt registry kulcsok jogosultságait.

Hasznos szolgáltatás, hogy script nemcsak a felhasználó be- és kijelentkezéséhez adható meg, hanem a számítógép indulásához és leállításához is. Ebben az az újdonság, hogy a beállítások egyszerűen kezelhető felületre kerültek ki, és nem kell a registry babrálásával vagy egyéb módon trükközni. A scriptek futtatásához a Windows 2000-ben alapértelmezésben megtalálható WSH (Windows Scripting Host) minden lehetőségét kihasználhatjuk, azaz scriptnyelvként használhatunk VBScriptet, JavaScriptet, vagy akár Perlt is.



1. kép: **A példaként használt három szervezeti egység és a Developer objektumai**

Szintén sokat használt megoldás lesz a könyvtár átirányítási (Folder Redirection) funkció, amellyel át lehet helyezni a felhasználó bizonyos könyvtárait, például az *Application Datát*, a *Desktopot*, a *My Documents-et* vagy a *Start Menu-t*. Például a My Documents mappát be lehet állítani a felhasználó saját hálózati könyvtárára (*\\servername\sharename\%username%*), így a dokumentumok a központi, naponta backupolt szerverre kerülnek. Azért is érdemes kihasználni az átirányítás lehetőségét, mert ellenkező esetben a dokumentumok a roaming profile részét képező könyvtárba kerülnének, amelyet minden egyes be- és kilépéskor át kellene másolni a szerverről a munkaállomásra, majd vissza. Ez jelentősen leterhelheti mind a szervert, mind a hálózatot, arról nem is beszélve, hogy nagyon lelassítja a be- és kijelentkezést.

A továbbiakban csak a registry-beállítással kapcsolatos lehetőségeket ismerhetjük röviden.

Active Directory és Group Policy

A Group Policy szorosan kapcsolódik az Active Directoryhoz, mivel a házirendet meghatározó GPO-kat az Active Directory containereihez, azaz a tartományokhoz és a szervezeti egységekhez tudjuk hozzárendelni. Csakúgy, mint az AD-t, a Csoportos Házirendet is menedzselhetjük távolról, mivel ez is „központi" helyen tárolódik.

MMC és Group Policy

Az NT alatt a policy file-t (NTCONFIG.POL, CONFIG.POL) a *Policy Editorral* kellett megszerkeszteni, majd a PDC *Export\Scripts* könyvtárában kellett elhelyezni, s ez átmásolódott a PDC és a BDC-k *Import\Scripts* könyvtárába. A Group Policy-t az IIS 4-ben bevezetett, és azóta az összes szervertermék esetében általánossá vált kezelőfelülettel – az MMC-vel lehet menedzselni a megfelelő snap-inek használatával. Az MMC-nek megvan az a nagy előnye, hogy tág keretek között lehet konfigurálni, és egységes kezelőfelületet ad a legkülönfélébb adminisztrációs feladatokhoz.

Policy létrehozára, jogosultság beállítása

A házirendi beállításokat házirend objektumokban (GPO) kell megadni, amelyeket ezután egy-egy tartományhoz, site-hoz vagy szervezeti egységhez rendelhetünk hozzá. Alaphelyzetben két előre elkészített policy áll rendelkezésünkre: az egyik a tartományra, ezt Default Domain Policynak hívják, a másik pedig a tartományvezérlőkre, ezt nem meglepő módon Default Domain Controllers Policynak nevezik. Ezen kívül, ha a gépekhez és/vagy a felhasználókhoz is szeretnénk házirendet hozzárendelni, akkor először létre kell hozni egy szervezeti egységet, majd pedig el kell hozzá készíteni a megfelelő házirend objektumokat.

Az *1. képen* három, általunk kreált szervezeti egység látható, a felső szinten elhelyezkedő GroupPolTeszt, valamint az alá tartozó Developer és Office. Az egységeket érdemes hierarchikus (fához hasonlatos) és/vagy listaszerű szerkezetet követve a cég valós szervezetének mintájára kialakítani. A Developer szervezeti egységhez két házirend objektum is kapcsolódik: a PolTesztDeveloper és a PolTesztDeveloperMore. Ahhoz, hogy a szervezeti egységeket és a házirend objektumokat módosítani tudjuk, megfelelő jogosultsággal kell bírnunk. Az objektum módosításához ráadásul nem elég az objektumon a megfelelő jogot beállítani, hanem NTFS jogokat is engedélyezni kell egy bizonyos könyvtárra – ez nem más, mint a SysVol megfelelő alkönyvtára, amelyet a későbbiekben mutatunk be. A policy azokon a számítógépeken, illetve felhasználók esetében érvényesül, akik hozzá vannak rendelve az adott szervezeti egységhez. Egy szervezeti egységhez több GPO-t is rendelhetünk szabályozható végrehajtási sorrenddel. A szervezeti egységbe természetesen csoportokat is felvehetünk, amelyek tartalmazhatnak számítógépeket vagy felhasználókat is. Ha az egységeket hierarchikusan helyezzük el, akkor alapértelmezésben az adott egység elérési útján elhelyezkedő összes GPO érvényre fog jutni, kezdve a Default Domain policyval. Ezen persze lehet változtatni, azaz blokkolhatjuk a hierarchiában feljebb elhelyezkedő beállításokat.

Végrehajtási sorrend

Könnyebb megérteni, hogy a számítógépekre és felhasználókra vonatkozó csoportos házirendek hogyan működnek, ha pontosan ismerjük ezek végrehajtási sorrendjét. E sorrend kötött, a rendszerindítás illetve a belépés folyamata során a következő:

- A számítógépre vonatkozó Group Policy végrehajtása, ez alapesetben szinkronizáltan történik. (Ez röviden azt jelenti,

hogy a gép megvárja, míg a GP beállítások kiértékelődnek, és addig nem tölt be mást.) Ha több GP is végrehajtódik, akkor ezek szintén bevárják egymást.

A végrehajtási sorrend során először a számítógépre beállított helyi házirend, majd ha a számítógép valamilyen domain része, akkor az ahhoz rendelt policy (pl.: a Default Domain Policy), végül a szervezeti egység(ek)hez hozzárendelt policy(k) hajtódnak végre. Mivel a számítógép több szervezeti egységnek is a tagja lehet, és mindegyikhez több objektumot lehet rendelni, többféle sorrendben, nagyon tág határok között konfigurálhatjuk a rendszert. Ez viszont azt a veszélyt is magában hordozza, hogy ha túlbonyolítjuk a hierarchiát, akkor jelentősen megnehezíthetjük a beállítások nyomon követését.

- Hálózati komponensek betöltése, majd elindítása (Remote Procedure Call System Service, röviden RPCSS, Multiple Universal Naming Convention, röviden MUP stb.).
- A startup script(ek) indítása – ez(ek) alapértelmezésben, a háttérben fut(nak) – szinkron módon. Mivel minden objektumhoz beállíthatunk egy-egy startup/shutdown scriptet, ezért ez esetben több script is lefuthat egymás után.
- Megjelenik a CTRL-ALT-DEL felirat, be lehet jelentkezni a számítógépre.
- A felhasználói név és jelszó megadása után a felhasználó azonosítása kezdetét veszi. Ha az jogosult a belépésre, akkor a beléptetési eljárás elindul.
- A felhasználói profil (User Profile) betöltése. Ha a felhasználónak van roaming profile-ja, akkor ez a megfelelő hálózati területről történik, ha nem, akkor a lokális profile-ból, ez pedig a *%SystemDrive%\Documents and Settings\%UserName%* alatt található.
- A felhasználói GP végrehajtása a számítógépéhez hasonlóan szinkronizált módon. A végrehajtási sorrend megegyezik a számítógép kapcsán leírt végrehajtási sorrenddel, azaz a helyi policy, domain policy, majd a szervezeti egység(ek)hez tartozó policy hajtódik végre.
- A logon script(ek) indítása – alapértelmezetten a háttérben – a felhasználói felülethez képest aszinkron módon. (Azaz a felület betöltése és a script(ek) végrehajtása párhuzamosan megy végbe.) Az objektumok scriptjeinek lefutása után legutoljára a felhasználó logon scriptje fut le, ez viszont normál ablakban, hasonlóan az NT-ken alkalmazott logon scripthez.
- A felhasználói felület betöltése.

Mint már utaltunk rá, be lehet állítani, hogy az alapértelmezéssel ellentétben a scriptek aszinkron módon fussanak le, illetve azt, hogy a kimenetük ablakban láthatóvá váljon. Az alapértelmezett beállítások azt a célt szolgálják, hogy a felhasználó minél kevesebbet vegyen észre az általa igényelt munkakörnyezet kialakításának folyamatából.

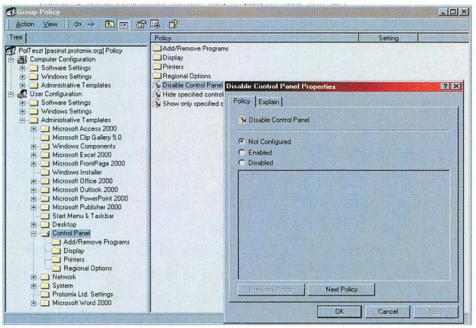
Beállítás

A következőkben a GP által teremtett beállítási lehetőségeket mutatjuk be, azon belül is a registry beállításokat, amelyek az Administrative Templates alatt találhatók meg. A másik két kategóriával itt nem foglalkozunk részletesebben: ezek az alkalmazások telepítését szabályozó Software Settings és a leggyakoribb beállításokat (scriptek, jogosultságok, könyvtárak) összefogó Windows Settings.

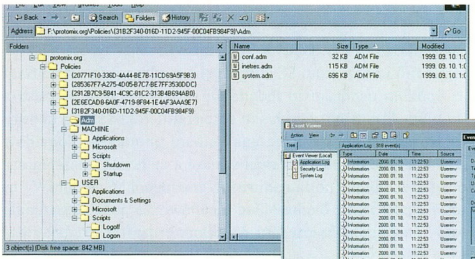
A *2. képen* látható, hogy az Administrative Templates alatt mely alkalmazásokhoz és operációs rendszer funkciókhoz találunk beállítási lehetőségeket. Látható, hogy például letilthatjuk a *Control Panelt*. A beállítási panelen minden esetben három lehetőség közül választhatunk: Not Configured, Enabled és Disabled. Ezen túlmenően attól függően, hogy az adott registry kulcs(ok)nak (REG_DWORD, REG_EXPAND_SZ, REG_SZ) milyen a típusa, további beállítható mezőket találhatunk (pl.: szövegbeviteli mező). Az Administrative Template alá szabadon berakhatunk saját készítésű template file-okat is.

Könyvtár és registry felépítése

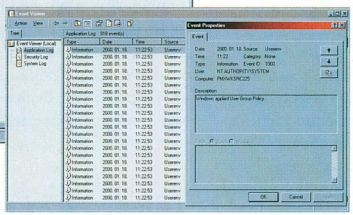
Ahhoz, hogy a csoportos házirendek által létrehozott file-ok (REGISTRY.POL, scriptek, administrative template-ek stb.) minden tartományvezérlőn elérhetőkké váljanak, olyan helyen kell elhelyezkedniük, amely rendszeresen szinkronizálódik a többi szerverrel. Ilyen a Windows 2000 alatt a SysVol könyvtár, ezt a tartományvezérlőnek konfigurált operációs rendszer automatikusan létrehozza, megosztja, és megfelelő jogokkal fel is ruházza. A csoportos házirendet is ebben a könyvtárban helyezték el a *%systemroot%\sysvol\<SYSVOL>\'full_domain_name'\Policies\GUID* útvonalon, ahol a <SYSVOL> a SysVol megosztás (share), a GUID pedig a Group Policy Object egyedi azonosítószáma és egyben a könyvtár neve. Ez például a következőképpen nézhet ki: {9CD455A8-6D90-436C-BFEF-BB75E2D24298}. Az azonosítószámot a Windows 2000 automatikusan létrehozza, és a GPO tulajdonságai között megtalálható, hogy mely szám tartozik hozzá. A GPO könyvtára alatt minden esetben további három könyvtár található: az Adm, a Machine és a User.



2. kép: **A Group Policyval elláthatóalkalmazások fája**



3. kép: **A policy könyvtárak felépítése**



4. kép: **Group Policy események az alkalmazásnaplóban**

Az Adm könyvtár ad otthont az Administrative Template (.ADM) file-oknak. Ezek segítségével lehet a registry-beállításokat a grafikus felületen keresztül változtatni. Ezek a file-ok a kiterjesztéstől eltekintve részben eltérnek az NT-n alkalmazott template file-októl, ezért azok itt egy az egyben nem alkalmazhatók. A microsoftos alkalmazásokhoz már vannak Windows 2000 alatt használható template file-ok (pl.: Office 2000), és valószínűleg a jövőben megjelenő vagy már meglévő alkalmazásokhoz is kiadnak ilyet. A saját fejlesztésű file-okat módosítani kell, vagy sajnos újra kell írni.

A Machine és a User könyvtár alatt található egy-egy REGISTRY.POL file, amely a policy által beállított registry-kulcsok bejegyzéseit tartalmazza. Ezen kívül egy Applications és egy Scripts könyvtár is fellelhető alattuk. Az előbbiben a szoftvertelepítés során használt .AAS file-ok vannak, az utóbbiban pedig a szükséges scriptfile-okat helyezhetjük el (startup script, logon script stb.). A könyvtár felépítését a *3. képen* követhetjük nyomon. A registryt a GP máshogy kezeli, mint az NT-s policyk tették.

Ahelyett, hogy az érintett kulcsot közvetlenül felülírná a kívánt beállítással a *HKCU*, illetve a *HKLM* alatt a *\Software\Policies*, valamint a *\Software\Microsoft\Windows\CurrentVersion\Policies* részbe és csak ide írja be a szabályozandó értékeket. E két elérési út tartalmát a Windows 2000 törli, ha az azt meghatározó házirend objektumot „nem konfigurált" állapotba állítjuk, töröljük vagy a gépet/felhasználót másik konténerbe tesszük át. Így a megszüntetett policy a későbbiekben nem fog érvényre jutni. A pontos hely csak azokat érinti, akik saját adminisztrációs sablonokat (.ADM file-okat) akarnak létrehozni, magát az elvet azonban érdemes ismerni.

Néhány ötlet a teszteléshez

A házirend az operációs rendszer betöltése során (computer policy) vagy a felhasználó belépése során (user policy) hajtódik végre, azaz hatásai csak ezután érezhetők. Ha a policyt teszteljük, és új kulcsot állítunk be, akkor rendes körülmények között, attól függően, hogy a computer policyban vagy a user policyban módosítottunk, a számítógépet újra kell indítani vagy a felhasználónak újra be kell jelentkeznie. Ez folyamat meglehetősen időrabló. Szerencsére a következő utasítással ki is kényszeríthetjük a policy végrehajtását:

secedit /refreshpolicy computer_policy
secedit /refreshpolicy user_policy

Ezzel a módszerrel azonban a scriptek nem hajtódnak végre, azaz sokszor mégis csak a hagyományos módszerrel (belépés, kilépés, újraindítás) tudunk tesztelni.

Alapesetben a számítógépeken nem látható, hogy mi történik a policy végrehajtása során. Ez teljesen rendben van, hiszen az az előnyős, ha a felhasználó nem szerez tudomást az őt ért korlátozásról. Tesztelés során, a hibák felderítése céljából viszont fontos lehet, hogy valamilyen módon (például naplózás) nyomon tudjuk követni a policy érvényre jutása során fellépő eseményeket. Mint már említettük, szerencsére ez is megoldható Windows 2000 alatt, méghozzá a következőképpen lehet ezt beállítani. A registryben létre kell hozni a következő kulcsokat, a hozzájuk tartozó adat típusa REG_DWORD, amelyet 1-re kell állítani, ha az adott területen be szeretnénk kapcsolni a naplózást.

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics\RunDiagnosticLoggingGlobal
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics\RunDiagnosticLoggingGroupPolicy

Ha ezt beállítottuk, akkor minden házirenddel kapcsolatos megjegyzést megtalálhatunk az *Event Viewer Application Log*-ban (a példa a *4. képen* látható). A tesztelés végén érdemes a fenti kulcsokat kikapcsolni (kitörölni vagy értéküket 0-ra állítani), mivel a naplózás meglehetősen sok bejegyzést hoz létre.

Összefoglalás

Az új rendszer megismerése a kezdetekben sok munkát igényel, de ha elsajátítjuk az új szolgáltatások használatát, a befektetett idő hamar megtérül.

Összességében a Windows 2000 GP-je a hálózatmenedzsmentben jól használható eszköz, nagymértékben segítheti a rendszergazdák és a helpdeskek munkáját, és így jelenősen csökkentheti a TCO-t.

Mutató

Windows 2000 Group Policy White Paper:
www.microsoft.com/TechNet/win2000/win2ksrv/technote/nt5policy.asp

A Windows 2000 fürtkezelése

A Windows 2000 Advanced Server és Datacenter Server lehetővé teszi, hogy szabványos PC-k felhasználásával alakítsunk ki olyan szervereket, amelyek az elektronikus kereskedelemben és az üzletileg kritikus nagyvállalati alkalmazásokban is megállják helyüket. Az ezekhez a felhasználásokhoz szükséges megbízhatóság és skálázhatóság elérésében fürtkezelési képességük kulcsszerepet játszik.

Fürtnek a szerverek világában azt nevezik, mikor fizikailag összekapcsolunk több gépet, és ezek működését úgy hangoljuk össze, hogy képesek legyenek közös feladatokat elvégezni. A legegyszerűbb fürtmegoldások csak azt teszik lehetővé, hogy ha az összekötött kiszolgálók egyike leáll (lefagy vagy elromlik), az automatikus hibakezelő folyamat (failover) azonnal átadja a kiesett kiszolgáló feladatát valamelyik társának. A fejlettebb fürtözési módszerek a hibakezelésen túl terheléselosztásra is képesek, azaz szét tudják osztani a kiszolgálandó feladatokat a gépek között.

Fürtök definíciója a Windows 2000-ben

A fürt egymástól független számítógépek olyan csoportja, amelyek közösen futtatnak néhány alkalmazást úgy, hogy az ügyfél és az alkalmazás felé egyetlen rendszer látszatát keltik. A számítógépeket fizikailag kábelekkel kapcsolják össze, logikai összehangolásukról pedig a fürtkezelő szoftver gondoskodik.

Az összekapcsolt gépek között terhelésmegosztást is végezhetünk, és hibakezelésre is lehetőség nyílik, ezáltal a fürt az egyedülálló gépnél jóval nagyobb üzembiztonságra és teljesítményre képes.

A Windows 2000 fürtkezelése folyamatos elérhetőséget, méretezhetőséget (skálázhatóságot) és karbantarthatóságot nyújt. Lássuk, mit is jelentenek ezek a fogalmak:

- **Folyamatos elérhetőség:** A gépek fürtözését azért találták ki, hogy ne legyen olyan központi erőforrás, amelynek meghibásodása a teljes rendszer leállásával jár. Az, hogy az alkalmazásokat több számítógépen oszthatjuk szét, lehetővé tesz bizonyos mértékű párhuzamosítást és hibavédelmet, valamint javítja az üzembiztonságot.
- **Méretezhetőség:** a fürt feldolgozási teljesítménye növelhető további processzorok vagy számítógépek hozzáadásával.
- **Karbantarthatóság:** a fürt egységes rendszer képét mutatja a végfelhasználók, az alkalmazások és a hálózat számára, továbbá egyetlen felületen keresztül, akár távolról is adminisztrálható.

A fürt két típusa Windows 2000-en

A Windows 2000 két fürtkezelési módszert ismer, amelyek külön-külön és együtt is használhatók. Azt, hogy melyiket érdemes választani, az adott alkalmazás igényei döntik el. A két megoldásra az *1. ábrán* láthatunk példát:

- **Fürt szerviz:**

E szolgáltatás elsődleges célja az, hogy hibavédelmet nyújtson az olyan alkalmazásoknak, mint például az adatbázisok, az üzenetkezelő rendszerek és file/nyomtatási szolgáltatások. Az Advanced Server két csomópontú, míg a Datacenter Server négy csomópontú hibakezelő fürtöt támogat.

• **Hálózati terheléselosztás:**
Ez a szolgáltatás elosztja az IP-n (Internet Protokollon) keresztül érkező forgalmat a legfeljebb 32 csomópontú fürt tagjai között. A terheléselosztás jóvoltából biztosabban működő és jobban skálázható internetes szerverek építhetők például weblapok, streaming média vagy terminálszolgáltatások kiszolgálására. Mivel ez a szerviz képes együttműködni a WMI-re (Windows Management Instrumentation) épülő felügyelő alkalmazásokkal, észrevétlenül beilleszthető a már létező webszerver-farm infrastruktúrába. A hamarosan megjelenő App-Center Server is jó hasznát fogja venni.

A fürtszolgáltatás értéke

Sok cégnél azonnal megáll az élet, ha az egyik levelező- vagy file-szerver kiesik. Nagyon fontos, hogy az üzlet működéséhez elengedhetetlen számítógépes szolgáltatások ne állhassanak le mindössze egyetlen hardver meghibásodása miatt. A fürtözés képes kiküszöbölni ezt az Achilles inat.

Ha ugyanis hardver- vagy szoftverhiba lép fel valamelyik csomóponton, akkor a fürtszolgáltatás az itt futó alkalmazásokat (több is működhet egyszerre) átirányítja valamelyik még működő csomópontra, és ott újraindítja őket. A fürtben résztvevő gépek közös merevlemezt is használhatnak (SCSI vagy Fibre Channel buszon), így a lehető legkevesebb adat vész el a hiba és a hibakezelés hatására.

A fürtszolgáltatás előnyei

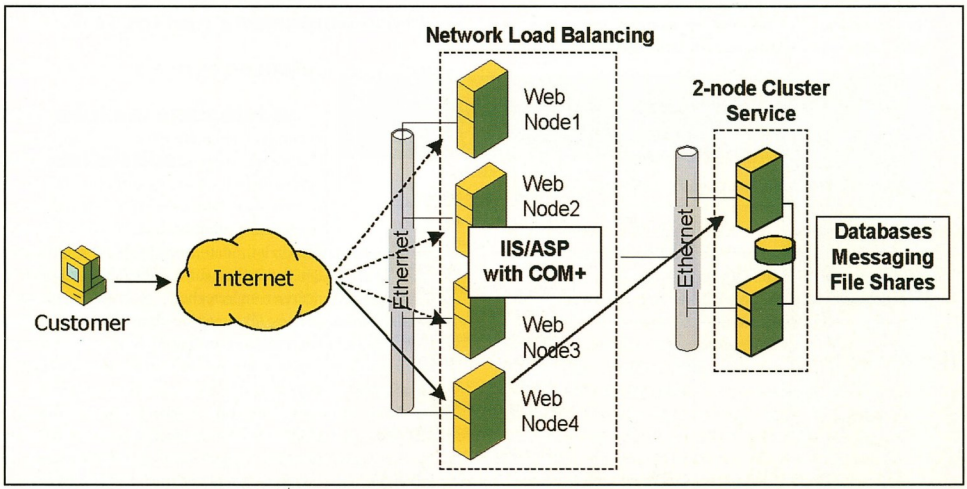
• **Lerövidíti a váratlan üzemszüneteket:** a hardver- vagy szoftverhiba által okozott leállás bevételkiesést és elégedetlen vásárlókat eredményezhet, ráadásul az informatikusok munkáját is feleslegesen gyarapítja. Ezekben az esetekben a közös merevlemezes fürtözés nagymértékben csökkentheti az üzemszünet hosszát.

• **Zavartalanná teszi a frissítéseket:** a fürtszolgáltatás lehetővé teszi, hogy a nélkül frissítsünk, hogy megzavarnánk a kliensek működését. A kiszolgálás leállítása nélkül cserélhetjük a hardverelemeket és a szoftvereket, sőt még operációs rendszert is.

Ehhez mindössze át kell irányítani az összes alkalmazást az egyik csomópontra, amíg a másikat módosítjuk. Ha jelenleg NT 4 Enterprise Edition-alapú fürtöt használunk legalább Service Pack 4-gyel, akkor leállítás nélkül frissíthetünk Windows 2000-re a fenti „rolling upgrade" módszerrel.

• **Továbbra is a jól bevált alkalmazások használhatók:** jelenleg is többtucatnyi fürtkész alkalmazás kapható a legkülönbözőbb célokra. Ezek között akadnak adatbázisok, mint a Microsoft SQL Server 7.0 és az IBM DB2; találhatók levelező-szerverek és rendszerfelügyelő eszközök, mint a Microsoft Exchange Server 5.5 és a Lotus Domino, valamint a NetIQ-féle AppManager; ezen kívül katasztrófa-helyreállító eszközök, mint az NSI Software DoubleTake 3.0-ja. Vannak ERP (Enterprise Resource Planning) alkalmazások, mint a SAP, a Baan, a PeopleSoft vagy a JD Edwards. A fürtözés a legújabb verzióban már DHCP, WINS, SMTP és NNTP kezelésére is képes.

• **Szabványos hardveren használható:** a Windows 2000 fürtözéséhez nincs szükség különleges, drága masinákra, elegendő néhány közönséges szerver-PC és mindennapi tároló-



1. ábra: **A két fürtkezelő módszer használata jellemző elektronikus kereskedelmi környezetben**

eszköz. Ezzel jelentős beruházásoktól kímélhetjük meg cégünket.

Végezetül, a Windows 2000 fürtszolgáltatását könnyebb beállítani és használni, mint a korábbi verziókban. A jelentősen továbbfejlesztett Telepítő Varázslónak köszönhetően a fürtszolgáltatás konfigurálása kevesebb, mint tíz egérkattintást igényel az első csomóponton, és kevesebb, mint négyet a másodikon. A további menedzselés is pofonegyszerű a MMC-be beépülő Cluster Administrator segítségével.

A hálózati terheléselosztás értéke

Az elmúlt években az Internet és a hozzá kapcsolódó technológiák (intranetek, extranetek és a rájuk épülő alkalmazások) robbanásszerűen elterjedtek. Ennek következményeként az igény egyre nagyobb a dinamikusan méretezhető webszerverekre. A hálózati terheléselosztásnak, a Component Services elosztott alkalmazás-támogatásának és a jobban skálázható IIS 5.0-nak (Internet Information Services) köszönhetően a Windows 2000 maradéktalanul ki tudja ezt szolgálni.

A hálózati terheléselosztás alkalmazásának előnyei:

• **További kiszolgálók hozzáadásával gyorsan és folyamatosan méretezhető webalkalmazások:** az igények növekedésének megfelelően a terheléselosztást alkalmazó fürt teljesítménye egy-egy gép hozzáadásával vagy lecserélésével kis lépésekben növelhető. Ráadásul egyedi, drága hardverre sincs szükség a terheléselosztás irányítására.

• **Megteremti a webhelyek folyamatos elérhetőségét:** mivel a hálózati terheléselosztással működő webszerverek kevesebb, mint 10 másodperc alatt képesek átvenni kiesett társuk szerepét, a vásárló vagy a böngésző ügyfelek sohasem kényszerülnek tevékenységük megszakítására, sem a tervezett frissítés vagy karbantartás, sem pedig a váratlan leállások következtében. Az olyan alkalmazásfigyelő eszközökkel, mint a Windows 2000 Resource Kit részét képező ClusterSentinel, a terheléselosztott fürtök könnyedén karbantarthatók.

• **Felkészülés a Microsoft AppCenter Server eljövetelére:** ha a Windows 2000 hálózati terheléselosztás szolgáltatásával építjük ki site-unkat, akkor – megjelenésekor – biztosan tudjuk majd telepíteni az AppCenter Servert is. Az AppCenter Server olyan rendszerfelügyelő, figyelő és replikációs szolgáltatásokkal bír, amelyek kiválóan kiegészítik a hálózati terheléselosztással ellátott webszervert. A program olyan karbantartó- és telepítési lehetőségeket is fog tartalmazni, amelyek kifejezetten a hálózati terheléselosztással működő fürtök képességeinek fokozására hivatottak.

További információk

Általános információk, esettanulmányok, Gyakran Ismételt Kérdések:
www.microsoft.com/ntserver/ntserverenterprise/exec/overview/clustering/default.asp

Nagy hozzáférhetőségű webhelyek létesítése Windows 2000-rel:
www.microsoft.com/ntserver/ntserverenterprise/deployment/planguide/highavailweb.asp

Microsoft Windows 2000 Advanced Server:
www.microsoft.com/windows/server/Overview/intro/advanced.asp

Melyik fürtkezelő módszert érdemes választani különféle alkalmazások esetén?

Módszer / Alkalmazás	Fürtkezelés	Hálózati terheléselosztás	Előnyök
Webkiszolgáló-farm		✓	✓Gyors kapacitásbővítés ✓Minimalizálja a site állásidejét
Terminál szolgáltatások		✓	✓Gyors kapacitásbővítés ✓Csökkenti a szerverhibák hatásait
File/Nyomtatási kiszolgálók	✓		✓Csökkenti a szolgáltatás állásidejét ✓Biztosítja a hibakezelés utáni adatkonzisztenciát
Adatbázis/Üzenetkezelés	✓		✓Minimalizálja az alkalmazás állásidejét ✓Biztosítja a hibakezelés utáni adatkonzisztenciát
Elektronikus kereskedelmi helyek	✓	✓	✓Gyors kapacitásbővítés ✓Minimalizálja a kiszolgáló/alkalmazás állásidejének hatásait

1. táblázat: **Mindkét Windows fürtkezelő módszer alkalmazása jellemző elektronikus kereskedelmi környezetben**

A két módszer együttes használata

A két fürtkezelő módszer együttes alkalmazásával jól méretezhető és nagy üzembiztonságú, n-rétegből felépülő elektronikus kereskedelmi site-ok készíthetők. Ha az első vonalban futó webszerver-farmon terheléselosztást alkalmazunk, a hátsó rétegben futó üzleti adatbázisokat pedig a hibavédelem érdekében fürtözzük, akkor csaknem lineárisan méretezhető, és ezzel együtt szerver- és alkalmazáseredetű hibákra érzéketlen rendszert hozhatunk létre.

Ha a hálózati infrastruktúrát is a legjobb szokások szerint a lehető legüzembiztosabbra építjük, biztosra vehetjük, hogy a Windows 2000 alapú internetes üzleti alkalmazások folyamatosan működni fognak, és könnyen, az igényeknek megfelelően méretezhetők lesznek.

A Microsoft Distributed File System (DFS)

Holpár Péter
pholpar@protomix.hu

A DFS lehetőséget ad a rendszergazdáknak hálózatuk szerkezetének optimálisabb kialakítására, emellett lehetővé teszi a terheléselosztást, továbbá növeli a hibatűrést is. A feladat elvégzését egyszerű adminisztratív felület és varázslók támogatják.
A következőkben áttekintjük a DFS jellemzőit, és megpróbálunk hasznos tanácsokkal szolgálni a kialakításához.

Minden hálózati adminisztrátor tapasztalhatta már azokat a nehézségeket, amelyek az erőforrásokra történő csatlakozás hagyományos módszere esetén merülnek fel. A félreértések elkerülése végett erőforrások alatt a network share-eket értem – szó szerinti fordításban ezek ugyan hálózati megosztást jelentenek, de igazán megfelelő magyar szó híján az erőforrás kifejezést használom a továbbiakban. Először is, mivel minden csatlakoztatott erőforrás az ábécé egyik betűjét igényli, a kliens korlátozott a létrehozható kapcsolatok számában. Másodszor, a felhasználónak – hacsak nem használunk login scripteket – számon kell tartania, hogy melyik szerver milyen hasznos erőforrást tartalmaz. Minden egyes szerver esetén, amelyen file-okat kíván elérni, külön kapcsolat – újabb betű felhasználása az ábécéből – szükséges.

A Microsoft Windows 2000 Serverben a már beépített elosztott file-rendszer megoldja ezt a nehézséget, sőt új szolgáltatásain keresztül számos egyéb hasznos dologra is képes. A DFS – ez nevének megfelelően elosztott file-rendszert takar – lehetővé teszi az adminisztrátorok számára, hogy a hálózaton bárhol megtalálható erőforrásokból egyetlen könyvtárszerkezetet hozzanak létre.

A felhasználók – természetesen a beállított jogosultságoknak megfelelően – bármelyik file-t elérhetik ebben a hierarchiában anélkül, hogy tudniuk kellene, hogy az egyes könyvtárak fizikailag hol, milyen rendszeren találhatók. A kliens automatikusan, a felhasználó számára észrevétlenül mindig a megfelelő szerverre kapcsolódik. Míg a felhasználó úgy látja, hogy egyetlen könyvtárszerkezetben keres vagy navigál, addig a háttérben különböző szerverek különböző erőforrásait éri el.

Ezzel a módszerrel a felhasználó csupán egy erőforrásra kapcsolódva valamennyi, számára szükséges hálózati erőforráshoz hozzáférhet, feltéve hogy ezeket a rendszergazda egyetlen DFS fába szervezte.

Az erőforrások DFS fába rendezése tehát mindenhol célszerű lehet, kivéve azt a ritka esetet, amikor a hálózaton csupán néhány egymástól független, kóbor erőforrás érhető el.

A DFS menedzselése

Azoknak, akik ismerik a Windows 2000 új adminisztrációs felületét, nem okozhat meglepetést az, hogy a DFS adminisztrálása a *Management Console*-on keresztül történik.

A megfelelő snap-in az *Administrative Tools* programcsoportban található, a neve önmagáért beszél: *Distributed File System*. Ezt a grafikus felületet használhatjuk a DFS-sel kapcsolatos valamennyi feladat végrehajtására: másolatkészletek (replikák), csomópontok (nódok) és DFS gyökerek készítésére. Mivel az eszköz a legtöbb feladathoz varázslókat használ, a DFS fa létrehozása és menedzselése igazán egyszerű.

A menedzselt DFS gyökerek az MMC konzol filerészeként tárolódnak, ezért a DFS fák kiválasztása után java-

solt a konzol elmentése, hacsak következő alkalommal nem akarjuk a munkát ismét a DFS gyökerekre való kapcsolódással kezdeni.

Új, már létező DFS fák felvételére az MMC konzolban a *Distributed File System* objektumra jobb egérgombbal kattintva, majd a *Display an Existing DFS Root...* opciót választva nyílik lehetőségünk. Ne feledjük, hogy a konzol elmentése csak az úgynevezett Authoring mód esetén lehetséges, tehát ha módosítani szeretnénk a megjelenített DFS-ek listáján, akkor eleve ebben a módban indítsuk a konzolt. Az *Administrative Tools* programcsoportban jobb egérgombbal kattintsunk a *Distributed File System* ikonra, és válasszuk az Author opciót. Mivel a DFS snap-in (ez tipikusan a *%SYSTEMROOT%\system32\DFSgui.msc* file) alapértelmezés szerint csak olvasható, ezért ha azonos néven kívánjuk elmenteni a szerkesztés után, akkor a megnyitást megelőzően a csak olvasható jellemzőt ki kell kapcsolni. Természetesen, ha az eredeti .MSC file-t nem kívánjuk módosítani, akkor más néven is elmenthetjük a változtatásokat.

A DFS gyökerek egymásba is ágyazhatók, vagyis az egyik szerveren létrehozott gyökér a másik szerver DFS fájában kapcsolatként szerepelhet. Ez a hierarchia egyben az elosztott adminisztrációnak is kedvez, mivel az egyes szintek menedzselése külön delegálható az MMC technológia segítségével.

Tervezés

Bár a DFS adminisztrációját az MMC snap-in jelentősen megkönnyíti, a jól strukturált könyvtárszerkezet kialakítása továbbra is rendszermérnöki feladat. Mielőtt belekezdenénk a megvalósításba, érdemes leülnünk és elterveznünk, hogyan szeretnénk alkalmazni a DFS adta lehetőségeket (aki már telepített unixos szervert, jó hasznát fogja venni a kötetek kialakítása során szerzett tapasztalatainak). Ha nem jól tervezzük meg az elosztott file-rendszert, az könnyen használhatatlan hierarchiát eredményezhet.

A DFS-rendszer tervezése során figyelembe kell vennünk az elosztott file-rendszer korlátait is. Bár a DFS fába újabb szerverek erőforrásait felvéve a DFS tárolókapacitása látszólag nő, valójában nem hozhatunk létre nagyobb file-okat, mint amennyi szabad hely van azon a fizikai lemezen, amelyen a DFS adott ága található.

Ennek az a magyarázata, hogy a file-ok nem lóghatnak át egyik erőforrásról a másikra, mivel az erőforrások a DFS fától függetlenül továbbra is elérhetők közvetlen módon. A DFS csupán egy könyvtárszerkezet részeként tünteti fel az egyes erőforrásokat, de a file-ok ettől függetlenül az erőforrásokon tárolódnak. Nyilvánvaló, hogy nem hozható létre olyan file, amelynek egyik fele az egyik erőforráson, másik fele pedig máshol található.

Talán a legfontosabb lépés a tervezés során a DFS gyökerének szánt partíció kiválasztása. Erre a célra olyan partíciót kell találnunk, amelyen elegendő szabad hely van. Újabb erőforrások hozzáadásával csupán alkönyvtárakat hozunk létre a DFS-ben, ezért a gyökér tárolókapacitása utólag már nem növelhető ezzel a módszerrel. Persze, ha minden adatot alkönyvtárakban tárolunk, akkor szükségtelen túl nagy partíciót lefoglalni erre a célra. Külön partíció kialakítása egyébként sem kötelező a DFS gyökér számára, de ne feledkezzünk meg arról, hogy minden folyamat, amely a partíción levő szabad helyet csökkenti, gyakorlatilag a DFS elől fogyasztja azt.

Természetesen ez fordítva is igaz, ezért érdemes alaposan megfontolni a külön partíción való tárolást.

Az a tény, hogy a DFS fát alkotó erőforrások látszanak azon a szerveren is, ahol erőforrásuk tartózkodik, zavaró lehet, mert a felhasználók a hálózaton böngészve ezeket is látják. Ezt elkerülendő, célszerű rejtett erőforrásokat használni. Ha több szerveren a hibatűrés és a terheléselosztás szándékával azonos funkciójú erőforrásokat hozunk létre – ezek az úgynevezett replikák –, akkor célravezető az erőforrásoknak ugyanazt a nevet adni. Ez a gyakorlat egyszerűsíti az adminisztrációt is.

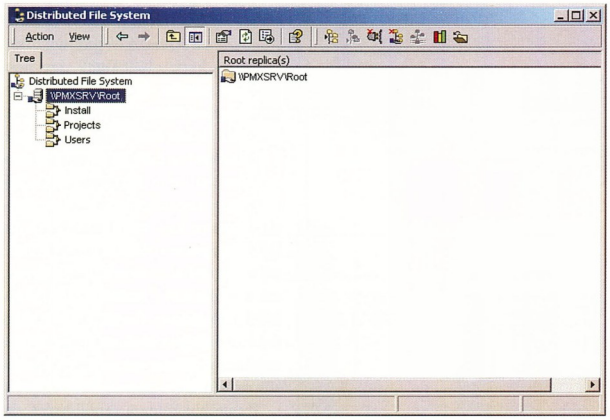
A DFS felépítése és jellemzői

A korábbi Windows verziókban alkalmazott rendszer esetén a felhasználó számos módon kapcsolódhatott az erőforrásokra. A legelterjedtebb módszer a hálózaton fellelhető számítógépek és a rajtuk található erőforrások böngészése volt. Ez az eljárás rejtett erőforrások esetén persze nem működik.

A másik, UNC-s (uniform naming convention) módszer is alkalmas erre a célra, ekkor a felhasználó az erőforrást a teljes elérési útjával adja meg, például a *Server* nevű gépen levő *Share* erőforrásra a *\\Server\Share* formában hivatkozik. Amennyiben az erőforrás rejtett, a név végére a $ jelet is oda kell biggyeszteni. Persze ennek a módszernek is megvan a maga – nem is kicsi – hiányossága: a felhasználónak név szerint kell ismernie a gépet és az erőforrást, amelyre kapcsolódni szeretne. Erre a tudásra általában úgy tesz szert, hogy az erőforrást megosztó rendszergazda megírja neki.

Bármelyik módszert használjuk is e kettő közül, a felhasználó számítógépe ugyanazokon a lépéseken keresztül kapcsolódik az erőforrásra: felveszi a kapcsolatot a távoli szerverrel, majd hozzáférést kér – szerencsés esetben kap is – a kiválasztott erőforrásra.

A DFS szintén erre a szerkezetre épít, de jelentősen rugalmasabb végeredménnyel. Vegyük a legegyszerűbb esetet. A rendszergazda létrehoz egy DFS gyökeret, ez éppen úgy viselkedik, mint a hagyományos hálózati erőforrási pont. Amikor azonban a felhasználó kiválasztja valamelyik alkönyvtárat a gyökérben, a kliensszámítógép észleli, hogy az nem valódi alkönyvtár, hanem mutató egy másik hálózati erőforrásra. A kliens ezt követően automatikusan arra a háló-



1. kép: **A DFS fát alkotó erőforrások különböző file-szervereken találhatók, a felhasználók számára mégis egyetlen hierarchiának látszanak**

zati erőforrásra kapcsolódik, ez akár másik gépen is lehet, és megjeleníti annak tartalmát.

Ez a szerkezet lehetővé teszi, hogy a felhasználók egyetlen DFS gyökéren keresztül a vállalat valamennyi file-szerverét elérjék *(1. kép)*. Ez a fajta DFS szolgáltatás már a Windows NT 4.0 Serverben is elérhető volt, ha telepítettük az ehhez szükséges rendszerbővítést. A kliens funkciók a Windows 98 és Windows NT 4.0-ban (beépítetten) megtalálhatók, a Windows 95 pedig ingyenes bővítés telepítésével alkalmassá tehető a DFS fák elérésére.

A Windows 2000 Server termékek továbbfejlesztett DFS szolgáltatást tartalmaznak. Az Active Directory használatával lehetőség nyílt arra, hogy a DFS gyökér-információ több szerveren keresztül is elérhető legyen.

A Windows 2000 kliensek az Active Directoryra kapcsolódva megszerezhetik az elérhető DFS gyökerek listáját, majd ez alapján automatikusan a földrajzilag legközelebbi – például az azonos site-on belüli – rendszerre kapcsolódnak, ily módon mérséklik a hálózati forgalmat. Ha a legközelebbi szerver nem érhető el, akkor a kliens automatikusan másik DFS gyökeret keres. Ennek hibatűrési, valamint terheléselosztási rendeltetése van.

Ugyanezeket a célokat szolgálja – csak más szinten – az a lehetőség is, hogy az alkönyvtárakról másolatokat (úgynevezett replikákat) hozhatunk létre más szervereken. A replikák közötti szinkronizációt a DFS replikációs összetevője végzi. Ezzel a módszerrel a DFS fa különböző részeihez eltérő szintű hibatűrő képességet rendelhetünk. A kliensek – az Active Directoryt felhasználva – a legközelebbi olyan szerverre kapcsolódnak, amelyen a keresett információ megtalálható.

Windows 2000 esetén a DFS fába nemcsak az erőforrásokat vehetjük fel, hanem az erőforráson belüli könyvtárszerkezet bármelyik mappáját is közvetlenül csatlakoztathatjuk.

Érdekes megfigyelni, hogy a szervernek abban a könyvtárában, mely a DFS gyökerét tartalmazza, valóban létrejönnek a könyvtárak, amikor kapcsolatokat veszünk fel a többi erőforrásra, és ezek neve megegyezik a kapcsolat nevével. Ha azonban megpróbálunk belépni ezekbe a könyvtárakba, „Access is denied" hibaüzenetet kapunk.

További érdekesség még az is, ahogy a rendszer kezeli mind a DFS által lefoglalt, mind pedig az elérhető szabad háttértárkapacitást.

Ha bármely DFS fát felcsatlakoztatunk távoli meghajtóként, és ennek jellemzőit megnézzük, akkor azt tapasztalhatjuk, hogy a szabad és elfoglalt terület mérete megegyezik a gyökeret tartalmazó partíció jellemzőivel. Eltérő eredményt kapunk azonban, ha a felcsatlakoztatott DFS fa gyökerében állunk, minden file-t és könyvtárat kijelölünk, majd megvizsgáljuk a jellemzőit. Ekkor ugyanis a DFS fa teljes hierarchiájában felhasznált fizikai tárolókapacitást kapjuk meg.

Fejlettebb és egyszerűbb adathozzáférés

A DFS fa használata nem korlátozódik a Windows 2000 Serverekre. Bármilyen Microsoft rendszer, amely alkalmas file-ok megosztására (például Windows for Workgroups, Windows 95, Windows 98 vagy Windows NT) – sőt, megfelelő szoftverek használatával még a NetWare, a Banyan, a Macintosh és a Unix-rendszerek is –, része lehet a DFS fának.

Ezek bármelyikén található erőforrások a felhasználó számára teljesen átlátszó módon elérhetők, például a gyökérben elindított keresés a teljes fahierarchiát végigkeresi, függetlenül attól, hogy az egyes könyvtárak mögött fizikailag található meghajtók valójában milyen operációs rendszert használó szerveren és milyen partíción találhatók.

Lehetőség nyílik akár arra is, hogy a szerverekben található CD-meghajtókat megosztva, és DFS fába szervezve virtuális CD-tornyot hozzunk létre, mindezt a felhasználók számára szintén észrevétlen módon. Nem minden rendszer alkalmas azonban DFS-kliensnek. Ez különleges szoftvert igényel, mivel a DFS gyökerében található könyvtárak legtöbbször csak kapcsolatok a fizikailag máshol található erőforrásokra, ráadásul a kliensnek esetenként több szerver közül

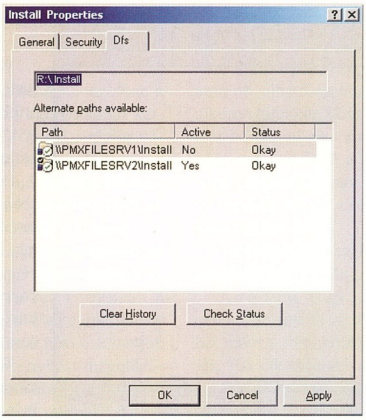
kell kiválasztania a legegyszerűbben elérhetőt.

Amint azt az előzőekben már említettem, a Windows 98 és Windows NT 4.0 tartalmazza a szükséges szoftvert, a Windows 95-höz pedig ez az összetevő ingyenesen letölthető. Ezzel együtt egy további korlátozással is találkozhatunk a Windows 95-ben, nevezetesen a bővítéssel ellátott Windows 95-kliens bejárhatja ugyan a DFS fát, de olyan részre nem léphet be, amelyhez a hozzá tartozó erőforrás a saját gépen található.

Hibatűrés és terheléselosztás

Azon túl, hogy a felhasználóknak egyszerűsített adathozzáférést tesz lehetővé, a DFS segít a hálózat hibatűrésének és terheléselosztásának megvalósításában is. Ehhez a rendszergazdáknak több Windows 2000 Serveren kell megosztaniuk ugyanazt a DFS gyökeret. Amikor a kliens a több szerver által megosztott DFS fára csatlakozik, az Active Directory értesíti a klienst, hogy milyen szervereken érheti el a megadott fát.

A kliens dönti el, melyik szervert választja. Ha a kiválasztott szerver nem válaszol, akkor a kliens automatikusan másikkal próbálkozik.



***3. kép:* A DFS fát alkotó könyvtárak – valójában külön erőforrások – jellemzői között a munkaállomásról ellenőrizhető, hogy az elérhető replikák közül a rendszer melyiket használja**

Mivel a kliensek több, azonos adatokat tartalmazó Windows 2000 szerverre kapcsolódhatnak, így nem egyetlen szerver szolgálja ki a teljes hálózatot, a DFS elosztja a terhelést a szerverek között *(2. kép)*.

Ráadásul a hálózati forgalom is csökken, mivel a kliensek az Active Directory segítségével a legközelebbi szerverre kapcsolódnak. Ezáltal a DFS egyszerre mérsékli a szerverek, valamint a hálózat terhelését. Amíg ezt a technikát alkalmazva a közelebbi file-szerver funkciók használata kisebb forgalmat hoz létre, addig a tartalom replikációja a szerverek között növeli a forgalmat.

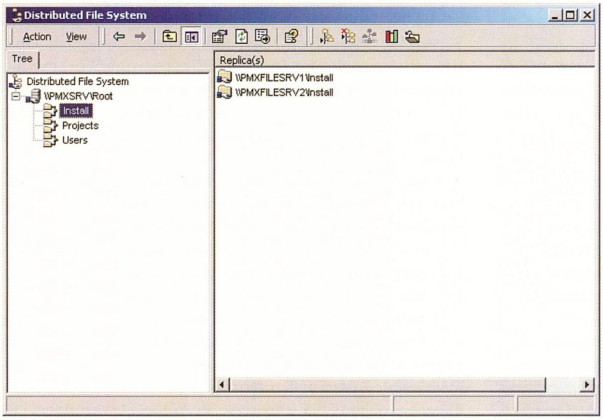
Ez utóbbi főleg a replikáció frekvenciájától függ, ennek optimalizálásával érhető el a legkedvezőbb eredmény. Nyilvánvaló, hogy ha az aktuálisabb információ a fontos, akkor gyakrabban, ha a forgalom csökkentése lényegesebb, akkor ritkábban kell replikálni.

A DFS fák alapvetően két üzemmódban működhetnek: hibatűrő vagy önálló módon. Hibatűrő módban a fa szerkezete valójában az Active Direcoryban tárolódik, és így automatikusan élvezi az általa nyújtott előnyöket, például az adatbázis elosztottságát. Az önálló DFS fák egy-egy szerverhez kötődnek, és ha az adott szerver leáll, akkor a DFS sem érhető el.

Azon túl, hogy önálló DFS fát csak azon a szerveren lehet elérni, amelyiken létrehozták, fontosnak tartom megjegyezni, hogy egy szerveren csupán egyetlen önálló DFS fát hozhatunk létre.

Amikor valamelyik kliens hibatűrő DFS-re próbál kapcsolódni, az Active Directory elküldi azoknak a szervereknek a listáját, amelyek a kiválasztott ág replikáját tartalmazzák. Ha az első szerver nem válaszol, a kliens addig próbálkozik a többivel, amíg sikerül valamelyikre kapcsolódnia.

A replikált hálózati erőforrások közötti átmenet teljesen átlátszó a kliensek számára, mivel a DFS elrejti a felhasználó elől a háttérben zajló folyamatokat. Amennyiben szükséges, a DFS fában szereplő könyvtár jellemzőinek megtekintésével a kliensről is ellenőrizhető, hogy az adott pillanatban a rendszer melyik replikát használja *(3. kép)*.

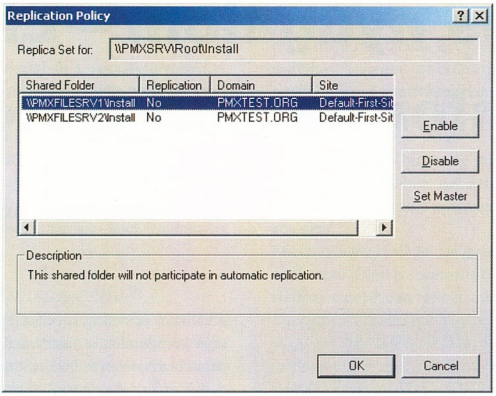


***2. kép:* A telepítőkészleteket tartalmazó erőforrás két szerveren is elérhető. Ha az egyik szerver leáll, a felhasználók automatikusan a másik szerverről érik el a file-okat**

A kliensek továbbra is képesek a hagyományos módon – az UNC útvonal megadásával – közvetlenül kapcsolódni a kiválasztott szerver DFS gyökerére, illetve valamennyi, a DFS fa részét képező könyvtárra.

A replikáció

A DFS-nek az a verziója, amelyet a Microsoft a Windows NT 4.0-hoz készített, ugyan már bírt a hibatűrő és terheléselosztó jellemzőkkel, viszont egy fontos lehetőség, a replikáció – ez az, ami előző kettőt igazán használhatóvá tenné – még hiányzott belőle. Valamilyen mechanizmusnak szinkronban kell tartania a több szerveren megtalálható adatokat, hogy a felhasználók mindegyik helyen ugyanazt az erőforrást lássák.



4. kép: **Replikációs beállítások – csak hibatűrő DFS esetén elérhető**

Szerencsére a Windows 2000 szerver már képes a DFS gyökerek és a csomópontok közti replikáció megvalósítására. A replikák készítéséhez a DFS snap-in használható. Replikákat csak a Windows 2000 NTFS-rendszerén hozhatunk létre, ugyanis FAT, FAT32 vagy Windows NT 4.0 NTFS partíciókon nem működnek.

A File Replication Service kezeli az azonos replikához tartozó erőforrások közötti adatszinkronizációt. Ez a szolgáltatás a lezárt és módosított file-okat automatikusan – alapértelmezéss szerint 15 percenként – szinkronizálja, tehát ez nem folyamatos, így arra nincs garancia, hogy az adat teljesen konzisztens legyen a replikán belül. Ezt a késedelmet – sajnos – kénytelenek vagyunk eltűrni.

A cache beállításai szabják meg, hogy pontosan mekkora késést engedélyezünk a szinkronizáció során. Ezt az értéket annak megfelelően állítsuk be, hogy a file-ok milyen gyakran változnak az adott replikában. Értelemszerűen ritkán változó adatok esetén nagyobb, a gyakran változók esetén pedig kisebb késedelmet célszerű beállítani.

Egyedi esetben elképzelhető az is, hogy az adatok olyan ritkán változnak, hogy automatikus replikációra nincs is szükség, a megosztott könyvtárak szinkronizációjáról a rendszergazda manuálisan gondoskodik, azaz a változtatásokat valamennyi erőforráson elvégzi.

Erre jó példát adnak a telepítő készleteket tartalmazó erőforrások, melyeket a felhasználók csak olvasási joggal érhetnek el *(4. kép)*.

A replikáció jellemzőinek beállítására csak hibatűrő DFS, azaz Active Directory használata esetén nyílik lehetőség. Ehhez kattintsunk a jobb egérgombbal olyan kapcsolatra, amelyhez legalább két replikát már létrehoztunk, majd válasszuk a *Replication Policy...* opciót. Önálló DFS vagy csak egy replikát tartalmazó kapcsolat esetén ez a menüpont nem érhető el.

A *Replication Policy* dialógusablakban *(4. kép)* kiválaszthatjuk, hogy a replikához tartozó könyvtárak közül melyek vegyenek részt az automatikus replikációban, és azt is, hogy ezek közül melyik az elsődleges kópia (azaz a master). Fontos megjegyezni, hogy adott szerveren található erőforrások között nem lehetséges automatikus replikáció beállítása. Ennek persze különben sem lenne sok értelme, hiszen sem a hibatűrést, sem a teljesítmény-elosztást nem szolgálná.

Integráció a Windows NT biztonsági rendszerével

Az erőforrások DFS fába szervezése nem befolyásolja az erőforrásszintű biztonsági beállításokat. Az egyes erőforrásokra beállított hozzáférési jogosultságok szabják meg, hogy a felhasználók hozzáférnek-e a DFS adott részéhez, vagy sem.

Amennyiben az erőforrás NTFS-partíción található, a jogosultságok file-szinten szabályozhatók, éppen úgy, ahogyan a hagyományos erőforrások esetén.

Ez lehetővé teszi például, hogy adott intézetben – ennek osztályain a file-szervereket külön rendszergazdák menedzselik – az egyes rendszergazdák maguk szabják meg a hozzáférési jogokat az erőforrásokra, azok mégis egyetlen DFS fában legyenek láthatók. Ezáltal megvalósítható az elosztott adminisztráció.

Összegzés

Az elosztott file-rendszer valószínűleg meg fogja változtatni a Windows-rendszerek hálózati működését. Segítségével a felhasználók az erőforrások egész hálózatát elérhetik anélkül, hogy a rendszer hálózati felépítését ismerniük kellene. Az Active Directory alkalmazásával a rendelkezésre állás is növelhető, ha több szerver között replikáljuk az adatokat.

A DFS Windows NT 4.0, Windows 95 és Windows 98 rendszerekkel is használható, így a jelenlegi rendszerek jelentős átalakítása nélkül is bevezethető.

Káosz és nyugalom – Életre hívott informatikai biztonság

Keleti Arthur, Kóbor Árpád, Nagy Zoltán
akeleti@icon.hu

Ki ne hallott volna a „félelmetes" hackerekről, a bárhová betörni képes crackerekről? A kasszasikerre törő, a tudományosság látszatát keltő filmek története gyakran az alábbi sémát követi: a „nem is olyan távoli" jövőben az okos, és persze jó oldalon álló ellenállók behatolnak a gonosz, ám informatikailag jól védett „multik" rendszerébe.

Az újságokban naponta olvashatjuk, hogy honlapokat törtek fel, pénzt vittek el az (addig) jó nevű bankból, vagy hogy a rendszer összeomlása miatt nagy szolgáltatóknál az ügyfélszolgálat szünetelt.

A „vírus" szó hallatán az influenza helyett ma már először az e-mail és a PC jut az emberek eszébe. Az olyan kifejezések, mint az „információ kiszivárgása", az „adatvesztés", a „távmunka" vagy az „elektronikus kereskedelem" aktív szókincsünk részeivé váltak.

Kaotikus állapotok uralkodnak? Tényleg ennyire bizonytalan a helyzet?

Vizsgáljuk meg, mi az oka a kialakult zűrzavarnak, és mihez kezdhet az, akinek feladata rendet tenni ebben a furcsa káoszban. Ha szétnézünk magunk körül a vállalatnál és a társadalomban, azt tapasztaljuk, hogy a szabályok korábbi rendszere megszűnt, a bizonytalanság pedig egyre nő az élet minden területén. Az ember, a vállalat, az ország igyekszik – amennyire lehet – megvédeni a saját környezetét, és fenntartani a szokott rendet. Minden és mindenki bizonytalan és bizalmatlan. Az értékrend átalakult.

Ma már nem elég az adott szó (a „gentleman's agreement"). Lehetőleg írásban, saját kezű aláírással kell véleményünket, szándékainkat közölnünk, és – biztos, ami biztos – még jobb, ha mindezt harmadik fél által megfelelően hitelesítjük.

Természetesen a vállalatok is az új helyzetnek megfelelően alakítják saját szervezetüket.

A vállalati informatikai rendszerek kiépítése többé-kevésbé megtörtént. A legfontosabb feladatot napjainkig főként az egyes alrendszerek, rendszerelemek integrációja jelentette. Az informatikai rendszer védelmével a vállalatok ez idáig nem sokat foglalkoztak. Az adatvédelem magától értetődően hozzátartozott az egyes megvásárolt részrendszerek kialakításához. Mindez (jobb esetben) jól átgondolt mentési rendszer bevezetését jelentette.

A szerteágazó, az informatikai biztonság minden elemét szem előtt tartó megközelítés, az ahhoz tartozó feladatok átgondolása mostanáig nem volt jellemző.

Mi a megoldás? Mi ellen kell védekezni, és hogyan védhető a vállalat információs vagyona? A továbbiakban ezekre a kérdésekre keressük a választ.

A hatékony védekezés elemei

A jól átgondolt biztonsági ügyviteli rend kialakítása (biztonságpolitika, szabályzatok, utasítások), illetve a felmért kockázatokkal arányos biztonságot garantáló informatikai eszközök kiválasztása tartozik e témakörbe.

Az informatikai biztonság megteremtése minden szervezetnél eltérő jellegű és mértékű ráfordítást igényel. Optimális megoldásról akkor beszélhetünk, ha a lehetséges veszélyek megelőzésére és elhárítására fordított erőforrások arányban állnak a fenyegető kár értékével. Miután a védeni kívánt területeket a fenti irányelvek alapján meghatároztuk, kialakíthatjuk a védekezés módját.

A hibás megközelítés

Hazánkban sajnos az a gyakorlat terjedt el, hogy a beszerzést nem előzi meg helyzetelemzés, veszélyforrás-kutatás, hanem a szervezetek a reklámok, a betörési hírek, valamint egyéb külső

befolyás hatására vásárolják meg a különböző informatikai biztonsági eszközöket.

A vevők gyakran nincsenek tisztában a veszélyforrásokkal. Nem tudják pontosan, hogy mit kell megvédeniük, ezért gyakorta a nem megfelelő eszközt választják ki. Ismert statisztikai adat, hogy a saját alkalmazott által elkövetett, illegális adatmanipuláció az információt legnagyobb mértékben fenyegető tényező. Ezzel szemben az is tény, hogy ma a cégek többsége a vállalati tűzfal beüzemelésével megoldottnak tekinti a biztonság kérdését.

Az így kialakított biztonság nem lehet sem kockázatarányos, sem költséghatékony.

Mi az informatikai biztonság célja?

Az IT-biztonsági rendszer célja az informatikai környezet szükséges biztonsági szintjének fenntartása a működtetés teljes életciklusa folyamán. Az IT-biztonsági koncepció a releváns fenyegetésekre összpontosítva költséghatékony védelem kialakítását teszi lehetővé.

Nézzünk egy példát! Az *1. ábra* állatorvosi lónak szánt vállalat vázlatán azokat a rendszerelemeket, amelyekről feltételeztük, hogy már léteznek, feketével jelöltük.

A kékkel jelöltek azok, amelyek a legtöbbször hiányoznak az informatikai biztonsági rendszerekből. A zöld szín a lehetséges távoli kapcsolatokat jelöli.

A továbbiakban a kép alapján lépésekre bontva fogjuk ismertetni, melyek azok az elengedhetetlen biztonsági megoldások, amelyek a teljes körű informatikai biztonsági rendszer kiépítéséhez szükségesek.

Router

A router a korszerű vállalat informatikai hálózatának „kapuja". Az ábrán az egyszerűség kedvéért csak az Internet felőli csatlakozásokat jelöltük, de nagyobb hálózatokban az egyes belső alhálózatok forgalmát is egy vagy több router irányítja.

Az informatikai biztonság szempontjából a routerek jelentik az első támadási felületet, amelyre csapás mérhető. Talán helyesebb így fogalmaznunk: a router a hálózati összetevők első fenyegetett eleme. E veszélyek forrása ugyanis nem feltétlenül a szándékosságból fakad.

A routerek sérülékenysége kiterjedt funkcionalitásukból következik. Napjaink informatikai hálózatain számos, különböző hálózati protokoll közlekedik. Ez egy sor felismerendő és betartandó szabványt, és egyúttal sok hibalehetőséget is jelent a router számára. A szabványtól eltérő protokoll-elemeket a routernek fel kell ismernie, és kezelnie is kell.

A router elsődleges feladata a beérkezett csomagok továbbítása, és nem azok vizsgálata, ezért nem könnyű megtalálni az egyensúlyt a pontos és gyors csomagtovábbítás, valamint az erőforrás-igényes csomagszűrés között. Természetesen a routerhez érkezett csomagok alapos kiértékelése elkerülhetetlen, de ahhoz, hogy ez simán történjen, céleszközök szükségesek.

Az informatikai biztonság szemszögéből nézve a routernek az alábbi fontos kívánalmaknak kell megfelelnie.

- Célhardver végezze a csomagszűrési, valamint továbbítási feladatokat.
  Ennek előnye: a megoldás gyors és pontos, jó eszköz esetén pedig hosszú távon is megbízható.
  Hátránya: nehezebb változtatni, javítani és upgrade-elni.
- Jó naplózási képessége legyen. Az informatikai rendszer biztonságát felügyelő személyek, valamint a szoftverek kielégítő mennyiségű és minőségű adathoz jussanak az áthaladó forgalomról. Ez segít felderíteni, illetve elhárítani a működés közben jelentkező hibákat.
- Könnyen menedzselhető legyen.
  Az esetleges meghibásodás vagy az informatikai struktúrában bekövetkezett változás ne okozzon túlzott mennyiségű adminisztrációt.

Tűzfal + DMZ (Demilitarizált Zóna)

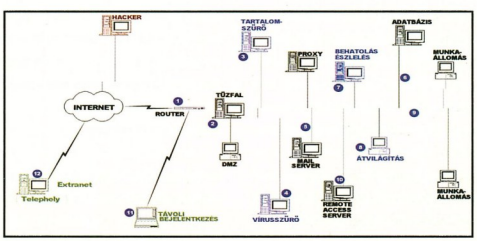
A tűzfal (pl.: RAPTOR Firewall/AXENT Technologies, Inc., GAUNTLET/Network Associates, Inc.) minden informatikai hálózat kritikus és alapvető biztonsági eleme. Az *1. ábrán* csak az Internet felőli csatlakozást jelöltük – mint a router esetében –, de természetesen tűzfalakat lehet és kell is telepíteni belső vállalati alhálózatok egymástól való elválasztására, illetve a köztük folyó kapcsolatok bonyolítása céljából.

A tűzfal feladata a hálózati protokollok ismeretét és a csomagok kezelését tekintve lényegesen kiterjedtebb, mint a routeré. Ezen kívül sokkal dinamikusabb és változatosabb is.

Éppen ezért a tűzfalak stabilan működő hardvereken és megbízható operációs rendszerekben futó (gyakran az operációs rendszert magát is megerősítő) szoftverek.

Az évek során az informatikai biztonsággal szemben támasztott igények a tűzfalak szerepét kiszélesítették.

A ma használatos tűzfalak minden egyes kapcsolatfelvételkor gondosan és alaposan megvizsgálják a hálózati forgalom különböző szintjeit.



***1. ábra:* Egy fiktív vállalat informatikai infrastruktúrájának biztonsági eszközei, szolgáltatásai**

Tartalomszűrő

Ugyan a behatolás elleni védelmet a tűzfalak teremtik meg, viszont az engedélyezett nyitott (HTTP vagy SMTP) csatornán keresztül áthömpölygő adattö-

meg még tartalmazhat olyan veszélyeket, amelyek ellen szintén védeni kell hálózatunkat. A veszély több irányból fenyeget: „támadásként" értékelhető üzenet nemcsak kívülről érkezhet, hanem belülről is kijuthatnak olyan bizalmas információk, amelyek nyilvánosságra kerülése sértheti a vállalat érdekeit. Emellett azonban nem szabad megfeledkezni a belső levélforgalomról sem (a levelek 70–80%-a), ennek szűrése is célszerű – bár ez látszólag a paranoia határát súrolja.

Ezekre a gondokra a tartalomszűrő eszközök szolgálhatnak megoldásul (pl.: MIMEsweeper/Content Technologies, Inc., WebShield/Network Associates, Inc.). Ezek a hálózati forgalmat szűrik, s a többségük ma már kiegészült vírusellenőrzéssel is. E programcsomagok általában gateway jellegűek: a teljes forgalomnak át kell haladnia rajtuk ahhoz, hogy hatásosan tudjanak dolgozni. Az SMTP, HTTP, FTP gatewayek a legjellemzőbbek.

Fontos tulajdonságuk még, hogy az e-mail forgalmat nemcsak szűrni, hanem irányítani is képesek. Intézkedhetnek például a bizonyos mérethatárt meghaladó elektronikus levelek késleltetett kiküldéséről, vagy a gyanús tartalommal bíró üzenetek karanténba juttatásáról.

A tartalomszűrő a levél szövegét vizsgálja, eközben rákeres bizonyos, előre meghatározott szavakra, illetve kifejezésekre.

A tartalomszűrőn fennakadó objektumokról folyamatos riasztást, illetve értesítést kaphatunk, s így szükségtelenné válik a naplófile-ok fáradságos és idegőrlő böngészgetése.

A tartalom vizsgálatát kiterjeszthetjük ActiveX objektumokra és Java appletekre is. Ezáltal a HTTP-forgalom szűrésébe azok a HTML-formátumban kapott levelek is bevonhatók, amelyek gyakran a címzett tudta nélkül veszik fel a kapcsolatot az e-mail küldőjével, vagy futtatnak le rosszindulatú programokat a címzett munkaállomásán.

A jó tartalomszűrők jellemzői:

- transzparens, automatikus működés;
- egyszerű illeszthetőség a meglévő cache-kiszolgálókhoz (a proxyhoz);
- strukturált, logikus és gyors konfigurálás;
- a hibakereső és -elhárító eszközök bőséges tárháza;
- független víruskereső;
- távoli menedzselhetőség;
- nagy teljesítményű, hatékony működés (az egyes modulok párhuzamos használatának köszönhetően).

Vírusszűrő

Napjainkban a „vírusirtók" fogalma már sokak számára ismerősen cseng. Ezek az eszközök megvédik számítógépes rendszereinket a rosszindulatú programokkal, vírusokkal szemben.

Mégis naponta hallunk olyan híreket, hogy számítógépes vírusok fertőztek meg hálózatokat, és hogy váratlan megjelenésük szolgáltatások működését és/vagy felhasználók munkáját nehezítette meg.

Hogyan történhet meg mégis, ha a vállalatnak vannak vírusellenőrző eszközei?

Egy biztos – soha sem lehetünk nyugodtak. Hiába telepítettük a legjobb eszközt, mindig újabb és újabb vírusok jelennek meg.

A megoldás olyan vírusellenőrző mechanizmus (pl.: NetShield/Network Associates, Inc., InterScan VirusWall/ Trend Micro, Inc, MIMEsweeper/Content Technologies, Inc.), amely összetett, valósidejű és központi irányítást tesz lehetővé. A vírusadatbázis automatikusan frissíthető, valamint az első szintű védelmet a gateway látja el, továbbá a desktopvédelem intelligens logelemzést hajt végre, proaktív, és értesíti a rendszergazdát, ha valamilyen rendellenes esemény történik. A rendszer leveszi a felelősséget a felhasználó válláról – desktopszinten, észrevétlenül működteti a vírusellenőrzést. Így az egységes, betartható és központilag felügyelt.

A munkaállomásokra és a szerverekre telepített vírusszűrők az adminisztrátor számára az ismert protokollokon keresztül (pl.: HTTP) könnyen menedzselhetők. A naplófile-ok elemzése, a vírusminták frissítése vagy a konfigurálás a központból történhet.

Mail-szerver

A központi mail-szerverek is számos külső és belső veszélyt rejthetnek A mail-szerverek által ma használatos protokollok jó része (akárcsak a HTTP) még azokban az időkben született, amikor az informatikai biztonság nem szerepelt az alapelvárások között. A POP3-szerver például könnyen válhat jelszópróbálgatás (brute force password attack) áldozatává, mivel a protokoll nem tartalmaz magas szintű IT-biztonsági elemeket.

Az ismert levelezőrendszerek jelentős része saját formátumot és protokollt használ a kliensekkel történő kommunikációhoz, valamint a levelek tárolásához. Ezek az egyéni (gyakran gyengén vagy egyáltalán nem dokumentált) megoldások megnehezítik a vírusok, valamint a rosszindulatú támadások érzékelését és elhárítását. Ilyen esetekben a levelezőrendszerekre közvetlenül kapcsolódó vírusirtók és behatolás-érzékelők alkalmazása a célravezető. Ezek a szoftverek ismerik a levelezőrendszerek (például a Microsoft Exchange) által alkalmazott sajátos formátumokat.

A kéretlen elektronikus levelek túlzott forgalma (spamming) a levelezőrendszerek másik nagy biztonsági gondja lehet. A nagy mennyiségben érkező spamek lelassíthatják a vállalat belső levélforgalmát, vagy akár meg is akadályozhatják, hogy a levelek eljussanak a címzettekhez. A levelezőrendszerhez csatlakoztatott vagy előtte „őrt álló" tartalomszűrő az automatikusan frissülő spamlisták és jellegzetes spamelemek ismeretében az ilyen, kéretlen levélforgalmat képes korlátozni vagy megszüntetni.

Adatbáziszerver

Az adatbáziszerverek informatikai biztonságának kérdése meglehetősen új téma, éppen ezért az adatbázis-hozzáférések és -mérések informatikai biztonsági háttere nem minden esetben megfelelő.

Az adatbázis-szerverek védelme kidolgozásakor különösen nagy gondossággal kell kezelni a DoS (Denial of Service – szolgáltatás megtagadása) támadásokat. Ezek olyan akciók, amelyek

szerverek vagy szolgáltatások teljes leállását okozzák, bár adatvesztés nem történik.

Sajnos, az informatika gyors fejlődése diktálta szoftverfejlesztési tempó gyakran a nagy biztonsági lyukak és a sérülékenység megjelenéséhez vezet. A fejlesztők nem minden esetben tudnak az informatikai biztonságra összpontosítani az összes szerver, szoftver vagy szolgáltatás tervezése során. A legtöbb DoS támadás ennek „köszönhető", ezért a nagy forgalmú és érzékeny adatokat tartalmazó szerverek védelme kötelező!

Az adatok integritásának és hitelességének a megőrzése az adatbázisszerverek működésében (különösen az érzékeny adatok kezelése következtében) kiemelt szerepet játszik. Ezért gondoskodnunk kell az adatbázisszerver és a kliensek adatkapcsolatának titkosításáról, valamint az adatbázishoz csatlakozó felhasználók erős azonosításáról, illetve hitelesítéséről. A PKI (Public Key Infrastructure – Nyílt kulcsú rendszer) alapú biztonsági megoldások sokat segíthetnek ebben. Az adatok kódolása általában szimmetrikus titkosítással, valós időben történik.

A megoldás gyors, és nagyságrendekkel csökkenti az adatok megváltoztatásának, illetve eltulajdonításának kockázatát. A felhasználók egyértelmű azonosítása és hitelesítése a felhasználóra jellemző, egyedi kulcs használatával szintén megoldható a PKI-alapú rendszerekben.

Behatolás-észlelés

Az esetleges behatolások folyamatos monitorozása az egyik további lehetséges védekezési mód a hackertámadások, valamint az illetéktelen hozzáférések ellen. Az úgynevezett „aktív biztonságot megvalósító eszközök" (pl.: Intruder Alert/AXENT Technologies, Inc., Real Secure/Internet Security Systems, Inc., CyberCop Monitor/Network Associates, Inc.) állandóan figyelik a rendszer biztonsági eseményeit, észlelnek minden gyanús tevékenységet, betörési kísérletet, és azokra riasztással vagy akár a hálózati kapcsolat megszakításával azonnal válaszolnak.

A különböző szerverekről összegyűjtött naplófile-ok és adatok kiértékelése rendszerint sok adminisztratív munkát igényel.

A korszerű behatolás-észlelő megoldások a különböző veszélyeztetett szerverekre (esetleg munkaállomásokra) klienseket telepítenek, ezekkel valósítják meg az adatgyűjtést, valamint az észlelt hálózati támadások, s az erre adott válaszok jelentését, illetve naplózását. A kliensek számos operációs rendszert támogatnak, s ismerik azok jellemző sérülékenységét is.

A legtöbb eszköz „minta" alapján működik – a mintanyelv meghatározza a támadásnak minősülő adatcsomagokat a hálózati forgalomban. Ez a mintanyelv általában nem nyilvános, és a gyártó rendszeresen frissíti.

Léteznek továbbá olyan kiegészítő eszközök is, amelyek a „mézesmadzag" módszerrel védik a hálózatunkat. Hamis reakciókkal és bemutatkozásokkal csábítják a külső (vagy belső) betörőjelölteket, s közben bizonyítékokat gyűjtenek ellenük.

Az ilyen rendszerek legnagyobb előnye az, hogy azonnal értesülhetünk az informatikai hálózatot ért támadási kísérletről, vagyis nem csak a bekövetkezett káreset kapcsán akadunk a behatoló nyomaira.

Átvilágítás

Tudatosítani kell, hogy a biztonság soha sem száz százalékos, és a helyzetkép mindig csak az aktuális pillanatot tükrözi. Az idő előrehaladtával újabb technológiák és veszélyforrások jelennek meg. A biztonság megfelelő szinten tartásához periodikusan felül kell vizsgálnunk IT-biztonsági infrastruktúránkat. Erre a szkenner eszközök (pl.: Internet Scanner/Internet Security Systems, Inc., NetRecon/AXENT Technologies, Inc., CyberCop Scanner/Network Associates, Inc.) a legalkalmasabbak.

Ezeket két csoportra oszthatjuk: a hálózatalapúakra és a hostalapúakra.

A hálózatalapú szkennereszközöket a kockázatelemzés, illetve az auditálás során használhatjuk – hatékony segédletet nyújtanak a teljes informatikai rendszer sérülékeny pontjainak feltérképezéséhez. Ezek az eszközök az átvilágítás során egyaránt figyelembe veszik a nemzetközi hackerközösség tapasztalatait, valamint a legfrissebb betörési technikákra vonatkozó elemzéseket. Segítségükkel a gyenge pontok és a konfigurációs hibák felkutathatók. Az átvilágítás során el kell végezni a hálózati eszközök, valamint a teljes kommunikációs folyamat auditálását. Az eredmény a helyzetjelentés, melynek alapján a lehetséges biztonsági lyukak sorra kiküszöbölhetők.

A hostalapú szkenner eszközök segítenek abban, hogy automatizáljuk a biztonsági stratégia megtervezését és megvalósítását, s a biztonságpolitikában megfogalmazott elvek érvényre juttatását. Lehetővé teszik a központi menedzsmentet, a felhasználóengedélyezést, a file-védelmet, és a jelszó hatékonyságának ellenőrzését. Folyamatosan vizsgálják a rendszer passzív beállításait (összevetve a „maszk" által rögzített előírásokkal), és rendszeres jelentést készítenek a rendszer pillanatnyi állapotáról.

A szkennereszközt (vagy eszközöket) a meghatározott irányelvek, illetve elvárások alapján kell telepíteni a kijelölt gépekre. Ezáltal a hálózat és a kritikus gépek, illetve szerverek átvilágítása, auditálása és monitorozása lehetővé válik.

Hálózat

A korszerű informatikai hálózatokon számos információ halad át. Az adatbázis- és levelezőszerverek, a proxyk, a munkaállomások mind-mind különböző protokollokat használnak, ezek jó része csak kis mértékben tartalmaz informatikai biztonsági elemeket. Legtöbbjük például nem használ titkosítást a hálózaton áramló adatok védelmére. Az informatikai biztonság kérdése azonban már az aktív és a passzív hálózati eszközök, vagyis az informatikai struktúra szintjén jelentkezik. Érdemes a kialakítandó vagy már működő hálózatainkat minél „lehallgatásbiztosabbá" tenni.

A cél, hogy a hálózatba kötött munkaállomásokról senki se figyelhesse (se külsős, se belső munkatárs) a titkosítás nélküli hálózati forgalmat, s ne gyűjthessen onnan adatokat, illetve felhasználói neveket és jelszavakat. Használhatunk jól konfigurált és admi-

nisztrált switcheket a hubok helyett, s ezzel már csomagszinten korlátozhatjuk az egyes gépek hálózati hozzáférését. Természetesen ezen túllépve az összes adatot titkosíthatjuk is, és a titkosított adatok forrásától (legyen az felhasználó vagy gép) megkövetelhetjük jogosultságának egyértelmű bizonyítását.

A fenti titkosítási feladatokra olyan szoftvereket érdemes használni, amelyek képesek az ismert hálózati protokollokra épülő gyors és valós idejű titkosítást, illetve azonosítást elvégezni akár hálózatunk belső tűzfalain keresztül, akár az Internet közegén át (PKI-alapú rendszerek).

RAS-kiszolgáló (Remote Access Server)

A RAS-kiszolgáló üzemeltetése lehetővé teszi, hogy adott számítógép távolról, telefonvonalon vagy más nagy távolságú, lassú vonalon keresztül kapcsolódjon a helyi hálózathoz. A kitűzött cél az, hogy a rendszerre kívülről kapcsolódó távoli számítógép a helyi hálózat részévé válhasson, s ugyanazokat a protokollokat, valamint szolgáltatásokat használhassa, mint amelyeket a helyi hálózatban lévő gépek (csak kisebb adatátviteli sebességgel). Ahhoz, hogy ez a kapcsolat létrejöjjön, RAS-szerver kell, amely a távoli bejelentkezést fogadja.

A RAS-szerverek már nevükben hordozzák az őket fenyegető veszélyek okát: a bejelentkezés nem helyi munkaállomásról történik. A felhasználó nincs fizikailag jelen az adott informatikai hálózathoz csatlakozó objektumok használata során. Ez felveti a felhasználó, illetve a távoli munkaállomás hitelességének kérdését. Ezekre az esetekre olyan erős felhasználó-hitelesítési megoldásokat érdemes „bevetnünk", amelyek egyértelműen és jól bizonyíthatóan azonosítják a hálózati jogosultsággal bíró felhasználókat. Ennek a feltételnek legjobban a PKI-alapú rendszerek felelnek meg. A felhasználók hitelességét garantáló kulcsok dedikált, a felhasználó adatait, jogosultságát is rögzítő chipkártyákon helyezhetők el. A kártyák megfelelő olvasóval távolról (pl.: otthonról) is alkalmazhatók a bejelentkező felhasználó „erős" hitelesítésére.

Ehhez a témához a virtuális magánhálózat (Virtual Private Network – VPN) fogalma is szorosan kapcsolódik. A VPN (pl.: RAPTOR VPN/AXENT Technologies, Inc., PGP VPN/Network Associates, Inc.) titkosítási megoldásokra épülő és megfelelő adatbiztonságot garantáló magánhálózat, amelyet mások által is használt, vagy nyilvános szolgáltató révén fenntartott infrastruktúrán (például az Interneten) hoznak létre. A VPN teljesíti mindazokat az adatbiztonsági, menedzselhetőségi, megbízhatósági, méretezhetőségi, valamint adatátviteli paramétereket, amelyek a hagyományos, belső hálózatokat jellemzik.

Távoli bejelentkezés (RAS-ügyfél)

A távoli bejelentkezés másik szereplője (a kiszolgáló mellett) a RAS-ügyfél, vagyis a kapcsolatot kezdeményező felhasználó. A kapcsolatfelvétel legtöbbször modem segítségével, telefonvonalon keresztül történik.

A támadások jó része nem technikai manőverek, hanem éppen a jelszavak megszerzésén alapul, ezért ahhoz, hogy megóvjuk informatikai rendszerünket a betörésektől, a lopásoktól, valamint az adatvesztésektől, nagyon fontos a bejelentkező szigorú azonosítása.

Az erős felhasználó-azonosítás (pl.: Icon Hydra Smart Card csomag/Icon Számítástechnikai Kft.) lehetővé teszi a felhasználó számára a biztonságos bejelentkezést és a szolgáltatások elindítását.

A kártyákon tárolható információ segítségével ellenőrizhető:
- hogy a felhasználó valóban az, akinek mondja magát,
- a szerver és a kliens valódisága,
- az információtartalom eredetisége,
- valamint az adatok hitelessége.

A felhasználónak tisztában kell lennie azzal, hogy a távoli bejelentkezés milyen kockázattal jár, ezen kívül ismernie kell a bejelentkezésre vonatkozó előírásokat.

Magához a bejelentkezéshez egyébként nem szükséges más, mint a kártya és a kártyához tartozó egyedi személyi azonosító kód (PIN-kód). Ezek segítségével a kártya használata során a felhasználó hozzáfér a számára engedélyezett erőforrásokhoz, illetve a szolgáltatásgazda is biztos lehet benne, hogy csakis az arra jogosult felhasználó éri el a rendszert (a részleteket lásd Hitelesség 2000 után című cikkünkben).

Extranet

Az extranet adott vállalat belső intranetkörnyezetének kiterjesztése telephelyeire, üzleti partnereire és egyéb rokon szervezetekre. Az így kialakított kapcsolattal olyan védett alkalmazásokhoz, szolgáltatásokhoz lehet hozzáférni, amelyeket egyébként az intranet kizárólag belső felhasználóinak nyújt.

A kapcsolat két, távoli intranet között felveti a felhasználó, illetve a távoli munkaállomás hitelességének kérdését. A telephelyek közötti biztonságos kapcsolatokat a VPN-megoldások teszik lehetővé. A VPN IP-alapú hálózati kapcsolatot jelent nyílt, nem titkosított vagy rejtjelezett formában.

Gyakori jelenség, hogy a gyártók a tűzfalszoftverek szolgáltatásait bővítik ki VPN funkciókkal. Érdemes továbbá olyan, erős felhasználó-hitelesítési megoldásokat használni, amelyekről korábban, a RAS-kiszolgáló esetében már írtunk.

Mi a teendő? Hogyan fogjunk a „nyugalom" megteremtéséhez?

A pontos helyzetfelmérés és kockázatelemzés után meg kell határozni azokat az irányelveket (az IT-biztonságpolitikát), amelyek alapján az egyes részterületek szabályozása megalkotható. Ennek gyakorlati alkalmazása az adott területek védelmét megteremtő eszközök konfigurálását is magában foglalja. Az ismertetett példában kiemelt területeken keresztül mutattuk be a védelem kialakításának gyakorlati megvalósítását nem feledve a megfelelő biztonsági rendszer működtetéséhez szükséges szabályozás (s annak érvényesítésének!) elsődlegességét.

A szabályozott háttérrel bevezetett informatikai biztonsági megoldások a káoszból nyugalmat teremtenek.

A Windows 2000 biztonsági szolgáltatásai

Fóti Marcell
marcellf@netacademia.net

Nehezen sikerült hozzákezdenem ehhez az íráshoz. Több napig gondolkodtam, milyen szempontok alapján válogassak a Windows 2000 biztonsági szolgáltatásai közül, de ennél sokkal nagyobb fejfájást okozott az, hogy milyen gondolatmenetre fűzzem fel ezeket.

Vajon elegendő lenne-e az Olvasók számára az, ha táblázatszerűen felsorolnám az összes újítást, s mindegyik mellé odaírnék egy-két dicsérő szót, vagy netán nevezzük nevén a gyermeket, és valljuk be: a Windows 2000 biztonsági újításait a Windows NT 4.0 biztonsági rendszerének gyengeségei kényszerítették ki? S még ha így is van, vajon hogyan fejezzem ki abbéli szent meggyőződésemet, hogy az NT 4.0 bizony a maga idejében igenis biztonságos volt, csak éppen a több millió eladott példány következtében ugyanolyan, ha nem nagyobb céltáblává alakult, mint a Unix operációs rendszerek? A Microsoft mindent elkövet a Windows NT 4.0 biztonsági réseinek betöméséért, gondoljunk csak a rendszeres Service Pack és Hotfix kibocsátásokra (magára vessen, aki nem telepíti a javításokat). S szóljak-e a hackerekről és a módszereikről?

Az élet aztán eldöntötte a kérdést. A legnagyobb hazai Internet-szolgáltatót ért egymást követő két hackertámadás fényében már nem lehet hiteles cikket a írni biztonsági kérdésekről, ha nem vesszük figyelembe azt a „szomorú" tényt, hogy új generáció „nőtt fel". Ennek tagjai a Sulinet által teremtett ingyenes Internetelérés segítségével nem várt tudásra tettek szert, ennek köszönhetően „gazdagabbak" lettünk a magyar hackernemzedékkel. Nekik már nem lesz újdonság, amit írok, annál inkább ismeretlen azonban a szakma „veteránjai", a húszas éveiket taposó jelenlegi rendszergazdák számára, akik csak lesnek, ha valódi támadás éri rendszerüket. Hiába, ebbe bele kell születni. Akkor tudjuk megfelelően használni a Windows 2000 új biztonsági szolgáltatásait, ha ismerjük a támadók fegyverzetét és harcmodorát. Ha az Olvasó e cikk hatására elgondolkodik hálózata biztonságán, és esetleg még a www.microsoft.com/security weblap böngészésére is rászánja magát, értő(bb) szemmel fogja szemlélni azt, amit lát. Ugyanis már lesz elképzelése arról, mit javít az a patch, amelyet például Buffer overrun támadás kivédésére lehet felhasználni.

Lopják az adatot!

Az információ napjaink gazdaságának igen fontos nyersanyaga, s mivel értékes alapanyag, ugyanolyan sokan vágynak rá, mint száz évvel ezelőtt az aranyra. Van azonban egy lényeges különbség az aranybányászat és az adatbányászat között, s nem a nyereségesség tekintetében: ez utóbbitól nem koszolódik össze a ruhánk. Ami a betöréses rablást és az adatlopást illeti, leleplezés esetén mindkettőért börtön jár. Emellett azonban nem mindegy, hogy az akció kivitelezése életveszélyes-e. Az adatlopáshoz ugyanis nem fegyver, hanem fotel, kávé és PC kell.

Ebből következően bankrablásra viszonylag kevesen adják a fejüket (az olyan macerás), mi viszont jobban tesszük, ha adataink védelméről átgondoltan gondoskodunk. Ehhez nem kell más, mint a kockázati tényezők, valamint a védekezési lehetőségek ismerete! A kockázati tényezők és a gyenge pontok feltárása céljából most pár percig gondolkodjunk hackerként! (Csak nehogy a kedves Olvasó úgy maradjon!)

Hack!

Induljunk ki abból az alapfeltevésből, hogy ismerjük a kitűzött célt, azaz tudjuk, hogy milyen adatot szeretnénk ellopni/letörölni/átírni.

Érdekes, hogy a cél eléréséhez (adatszerzés) is számos információra van szükségünk! Sok-sok apró adatmorzsa összegyűjtésével esetleg már tervet is kovácsolhatunk, de ennek ki-

vitelezése során bizony sokszor falakba ütközhetünk, és kezdhetünk mindent elölről.

Új információk, új terv, új kísérlet: ez mindaddig ismétlődik, amíg a hacker el nem éri kitűzött célját. Óriási hiba azt hinni, hogy mindez a szemünk előtt zajlik, és a hacker napokig lóg a hálózaton. Bizonyos információk megszerzéséhez nem is kell számítógép, elég lehet egy telefonhívás is. A feltört hálózatok mindegyike esetében emberi mulasztások tömege nyitja meg az utat a hacker előtt, más kérdés, hogy a mulasztást lehet, hogy nem is a felhasználó, hanem a szoftvergyártó követte el... Nézzük meg, hogy hackerünk milyen terveket készíthet annak megfelelően, hogy milyen messze jár a céljától!

a. terv – A hacker a tűzfal túlsó végen szomorkodik. Be kell jutnia belülre. Ehhez a tűzfal nyitott portjait és szolgáltatásait kell kipuhatolnia, illetve megkeresni a gyenge pontjaikat. Ez bizonyára roppant homályosan hangzik, ezért íme egy példa: beküldhet Micikének egy e-mailt (hamis feladóval, valamelyik munkatárs nevében). Ennek a csatolt dokumentuma olyan programocska, amely az engedélyezett tűzfalportok valamelyikén keresztül kommunikál a hackerrel. Legyen, mondjuk, a program neve TUZIJATEK.EXE, és Micike biztosan elindítja! Mivel a Windows 2000 nem tűzfal, az ilyen jellegű támadások elhárítását bízzuk szakemberre.

b. terv – A hacker akár fizikailag (mert a támadó az egyik kollégánk), akár távolról, de már bent van a hálózaton. Ilyenkor a hálózati forgalom elkapása-lehallgatása értékes adatokhoz juttathatja a figyelmes szemlélőt. A hálózaton áthaladó FONTOS.DOC, FIZETESEK.XLS éppúgy olvasható, mint a gyengén titkosított (LanMan, NTLM) vagy kódolatlan jelszavak (FTP, Telnet)! További tippekkel nem szolgálnék.

c. terv – A hacker fizikailag hozzáfér a célgéphez. Odasétál, és kikapcsolja. A leállított Windows olyan védtelen, mint a ma született bárány.

d. terv – A hacker be tud jelentkezni a célgépbe, vagyis ismer megfelelő nevet és jelszót. Nem nagy baj, ha ez az account „gyenge", azaz egyáltalán nincs rendszergazdai joga, mivel ezután már csak fel kell emeltetnie a jogosultságát, és rögtön a célegyenesben van! Erre is akad egy-két trükk, például ügyesen becsapja a rendszergazdát, hogy az futtasson le olyan batch file-t, amely kinevezi őt rendszergazdává. Ezúttal sem a tippzuhatag a lényeg, hanem a hacker gondolkodásmódja! Ne hagyjuk, hogy a végrehajtható file-okon bárki módosítást végezzen!

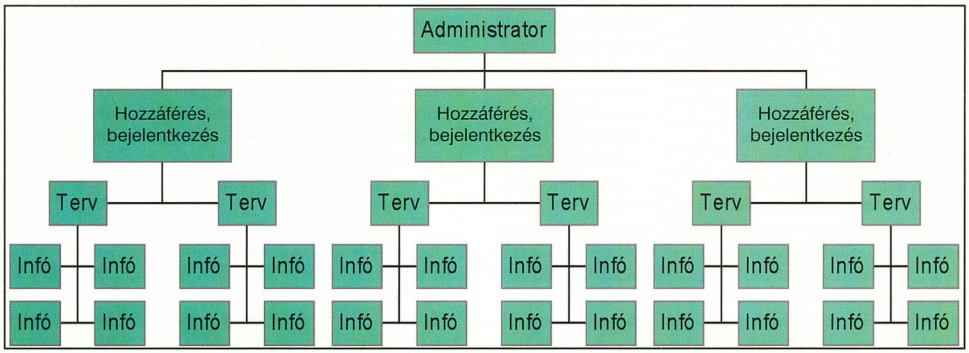
e. terv – A hacker már Administrator. Sajnos. De mit akarhat még? Nem ez a csúcsok csúcsa? Az Administrator mindent megtehet, még azt is, amit NEM (lásd Take Ownership)! Biztosan furcsán hat, de még van hová fejlődnünk. Valószínűleg Olvasóink is találkoztak már olyan zugokkal a regisztrációs adatbázisban (SAM), amelyeket a rendszergazda is csak úgy érhet el, hogy előtte jogosultságot ad magának, vagy „eltékeli az ownershipet". Van azonban „valaki", aki valóban mindenhova bejáratos: a SYSTEM nevű felhasználó! Hogy milyen módon lehet SYSTEM-ként bejelentkezni? Van erre is megoldás...

A hacker fegyvertára

A következő szakkifejezések a hacker szerszámosládájának darabjait takarják: Cracker, Sniffer, Backdoor, Buffer overrun, Denial of Service, Trojan, Replay, Hijack és még sok egyéb „hasznos" célszerszám, melyek mint a tolvaj álkulcsai, segítik a támadót céljai elérésében.

• **Cracker** – jelszófeltörő program. Ilyesmit vagy írni kell, vagy le kell tölteni, hiszen némi keresgéléssel minden fellelhető az Interneten. Írni lényegesen bonyolultabb, mert ehhez a hackernek ismernie kell a jelszavak titkosítási algoritmusát, valamint a célgép operációs rendszerét, továbbá a C programozási nyelvet. Ennyi tudás ritkán összpontosul egyetlen emberben.

• **Sniffer** – hálózati forgalomelemző és értelmező program. Számtalan sniffer létezik, a „hivatalos" változatok általában



1. ábra **A hacker szokásos kínlódása az áldozat megközelítésére**

valamilyen hálózat-felügyeleti eszköz részeként vásárolhatók meg, vagyis igen drágák. Szerencsére a Windowsban van ingyenes sniffer (Network Monitor), de üröm az örömben, hogy „egygépesre" butították, azaz idegen gépek közötti hálózati forgalom elkapására alkalmatlan. De hadd ismételjem meg: kis keresgéléssel minden fellelhető az Interneten!

• **Backdoor** – hátsó bejárat. Ez általában olyan hiba, amely a megcélzott operációs rendszerben rejlik, és lehetővé teszi, hogy valaki úgy jusson jogosultsághoz, hogy senki, még maga az operációs rendszer se vegye észre. Klasszikus backdoor-példa a GETADMIN.EXE – ezt azonban valamelyik javítócsomag már réges-régen hatástalanította –, amely az egyik Windows NT API hívás hibáját kihasználva lehetővé tette, hogy a közönséges felhasználó áthelyezze magát az Administrators csoportba. De backdoor a gondosan elrejtett apró programocska, vagy felhasználói név is, amellyel a hacker újra és újra rendszergazdaként térhet vissza.

• **Buffer overrun** – veremtúlcsordítási trükk. Ennek használata már komoly programozói ismereteket feltételez. A hacker erőfeszítése arra irányul, hogy a célgép operációs rendszerében olyan programozási hibát találjon, amelyet kihasználva valamely meghívott függvény („megfelelő" paraméterezés esetén) nem azt hajtja végre, amire való, hanem a hacker által megadott tetszőleges kódot. Ehhez persze az is kell, hogy az adott függvény hibás legyen, ebből következően úgy „nyelje le" a hacker kódját, mint a kacsa a nokedlit.

• **Denial of Service** – szolgáltatásmegtagadás. Ilyenkor a hacker célja az, hogy a kiszemelt áldozat gépén rendszerösszeomlást idézzen elő. Ez két fontos célt szolgálhat: az egyik, hogy csődbe viszi valamelyik elektronikus kereskedőt (például a karácsony előtti napokban elérhetetlenné téve szerverét), a másik, hogy rábírja a gyanútlan rendszergazdát a gép újraindítására. Ekkor a hacker által korábban odatelepített szerviz végre el tud indulni. Hogyan telepít bármit is a távoli gépre? Természetesen megbíz ezzel valaki mást! Ehhez pedig szüksége van…

• **Trojan** – trójai faló. Kívülről ártalmatlannak látszó programocska, ha azonban elindítjuk, egyáltalán nem azt teszi, mint amire számítottunk! Én .EXE kiterjesztésű e-mailcsatolást akkor sem indítok el, ha maga Bill Gates küldi.☺ A Back Orifice nevű „távmenedzsment" eszköz a trójai falovak klasszikus példája.

• **Replay** – visszajátszás. Miért is fárasztaná magát hackerünk a bejelentkezési jelszavak kódolásának visszafejtésével, ha snifferrel egyszerűen elkaphatja mások sikeres bejelentkezését a hálózaton, ezt azután némi kozmetikázás után vissza tudja küldeni; s bármily meglepő, beengedik! Szerencsére a Windows összes bejelentkezési módszere replay-álló (Challenge-Response, Kerberos)! Marad a bejelentkezés utáni forgalom visszajátszása. Ez akár valamelyik SQL-lekérdezés megismétlése is lehet!

• **Hijack** – eltérítés. Ez általában a TCP-csatorna eltérítését jelenti. Például oly módon, hogy a kész, felépített és azonosított, valamint hitelesített TCP-csatornát a hacker egyszerűen kicsavarja a jogosult felhasználó kezéből, de a kiszolgáló felé mosolyogva küldi tovább a kéréseket, az meg mit sem sejtve válaszol. Ez nagyon nehéz, összetett műveletsorozatot igényel: snifferrel össze kell gyűjteni a kapcsolat információit, beugrani a TCP-csatornába, és ezzel egyidejűleg Denial of Service támadással el kell némítani az eredeti felhasználót. Mindezek pontos időzítése és hibátlan kivitelezése a lehetetlenséggel határos. A hijack támadás alesete a „The man in the middle" támadás: ekkor a hacker a két egymással kommunikáló fél közé épül be úgy, hogy mindkettővel ő kommunikál, azaz minden forgalom áthalad rajta, így meg tudja hamisítani mind a parancsokat, mind pedig a választ. Nem könnyű...

A Windows 2000 rendszer biztonsági újdonságai

Először is emlékezzünk meg a Windows NT 4.0 tavaly decemberi eredményeiről: hálózati kártya és floppy-meghajtó egyidejű jelenléte esetén is viselheti a C2-es biztonsági tanúsítványt. Ez az igazolás ha nem is garantálja, de legalábbis lehetővé teszi, hogy az operációs rendszer elérjen bizonyos amerikai kormányzati körök által előírt megbízhatósági szintet. Sajnos, a C2 minősítést a gyártónak minden egyes operációs rendszer minden egyes javítókészletén külön el kell végeztetnie, így a Windows 2000 e díszes okmány nélkül kerül a piacra – de ami késik, nem múlik. Tekintsünk át néhány közismert C2 követelményt!

Kötelező bejelentkezés: a Windows 2000-ben ugyanúgy, mint az elődjében a felhasználók csak kötelező bejelentkezés után használhatják a számítógépet. Ez ahhoz szükséges, hogy a Windows tudja, kivel áll szemben, azaz a dolgozó melyik erőforrásokat használhatja, s melyeket nem.

Saját adatok feletti rendelkezés: ha a Windows 2000-ben bármilyen objektumot létrehozunk, annak tulajdonosává válunk. A tulajdonos pedig önállóan rendelkezik adataival – akár még a rendszergazdát is megfoszthatja a dokumentum kezelésének jogától. (De, mint már említettük, a rendszergazda mindent megtehet, még azt is, amit nem...)

Naplózási lehetőség: az operációs rendszerben zajló folyamatok (szinte) mindegyike naplózható. Ez lehetővé teszi, hogy az adatok visszamenőlegesen is hozzáférhetők legyenek fontos file-jaink használatáról, vagy például a hibás hálózati bejelentkezésekről. Nem szabad túlzásokba esni, ha rosszul választjuk ki a jegyzetelendő események körét, az eseménynaplózás teljesítménycsökkentő hatása igen jelentős lehet!

Objektumok újrafelhasználásának tilalma: ha adatainkat biztonságban szeretnénk tudni, nem elég magát az adatfile-t védeni, hiszen amikor például megnyitunk egy dokumentumot, akkor annak másolata bekerül a szövegszerkesztő által használt memóriablokkokba is. Ha kilépünk a szövegszerkesztőből, természetes igény, hogy a felhasznált memória ne csak felszaba-

duljon, hanem a tartalma is törlődjön, hogy a később indított alkalmazások semmiképpen se találkozzanak bizalmas dokumentumunk roncsaival, amikor memóriablokkot kérnek az operációs rendszertől. Az újrafelhasználás tilalma elvileg az átmeneti munkafile-ok, illetve a lapozó file tartalmára is vonatkozik. A gyakorlatban azonban ezt szinte lehetetlen garantálni, gondoljunk csak a hirtelen fellépő áramszünetekre, amelyek jótékonyan törlik ugyan a memória tartalmát, de egyszersmind lehetetlenné teszik a lapozó file gondos kitakarítását.

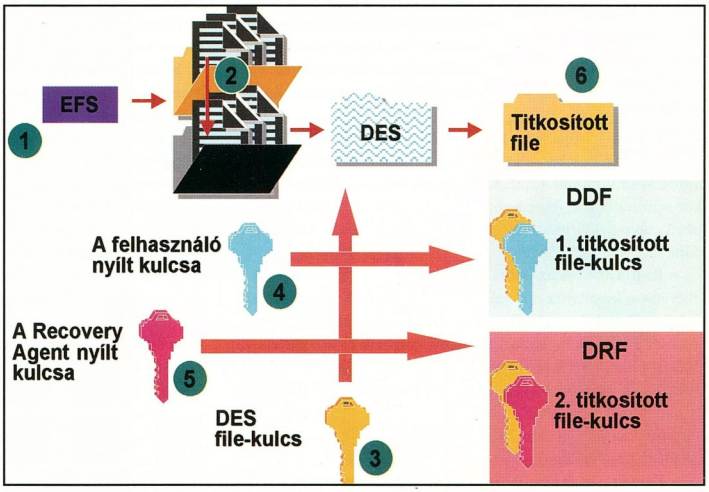
Windows 2000 felhasználói fiókok és csoportok

Kezdjük a csoportokkal: a hagyományos globális és helyi (local) csoportokon kívül két további típus jelent meg a Windows 2000-ben, az úgynevezett univerzális és a tartománybéli (domain local) csoport. Feltételezem, hogy az eddig is meglévőket mindenki ismeri, ezért csak a két újdonsággal foglalkozom. Az univerzális csoport a régi globálishoz hasonló, csak még annál is teljesebb: nemcsak mindenhol, de akár távoli, megbízotti tartományokban is felhasználható, sőt tagságát is akármelyik tartományból összeválogathatjuk. A tartománybéli csoport pedig felváltja a tartományvezérlők helyi csoportjait, amelyek eddig minden kezdő Windows NT gurut a sírba vittek. Az lenne a helyi csoport, amely mindegyik BDC-n megjelenik, de a munkaállomásokon nem? Az új tartománybéli csoportok tiszta vizet öntenek a pohárba: minden olyan csoport, amelyet tartományvezérlőn hozunk létre, automatikusan elérhetővé válik a tartomány összes számítógépén.

További újdonság, hogy a Windows 2000-ben végre nem kell minden a hálózaton is tevékenykedő szerviznek minden gépen külön felhasználót létrehozni. Vegyünk egy példát: NT-s rendszerben ha adott víruskereső programot mondjuk a vállalat mind a 100 kliensén szervizként futtattunk, akkor a vírusadatbázis központi frissítése gondot jelenthetett. Ugyanis, ha a munkaállomásokon futó szervizek nem kaptak saját nevet és jelszót (márpedig kiemelkedően szorgalmas rendszergazda híján szinte biztos, hogy nem), akkor „Local System" fiktív felhasználó névvel futottak. Amikor ezek hálózati kapcsolaton keresztül megpróbálták leszedni az egyik központi kiszolgálóról a frissítést (ez nyilván gazdaságosabb és biztonságosabb megoldás, mint hogy mindegyikük külön-külön szedje le az Internetről), akkor a szerveren Anonymousnak látszottak. Így a kiszolgálón Everyone csoportnak kellett (legalább read) jogot adni az adatbázis elérésére. Ám az Everyone jó tág csoport (Domain Users +Guest+Anonymous). Ez biza biztonsági rés! Aki nem tudott együtt élni ezzel a veszéllyel, az szépen körbejárhatott, és mind a 100 gépen hozzárendelhetett egy felhasználói nevet a szervizhez. Windows 2000-en ezt az egynapos kimerítő szellemi munkát megspórolhatjuk mindössze egyetlen kattintással, amelynek során megadjuk, hogy melyik gépen engedélyezzük, hogy a névtelen szolgáltatások a gép nevét és jelszavát (computer account) használják bejelentkezésre.

Védekezés a támadások ellen

Kezdjük a sort a merevlemez és az NTFS jogosultsági rendszere elleni támadásokkal. Közismert talán, hogy az NTFS jogrendszere addig megkerülhetetlen, amíg a jogosultságok rendőre, a Windows NT fut. De jaj annak a merevlemeznek, amelyet már nem őriz futó operációs rendszer: ugyanis akár másik NT-vel is elolvashatjuk róla az adatokat. A Windows 2000 jelentős fejlesztésen ment keresztül az ilyen jellegű gondok elkerülése céljából. Az NTFS5 lehetővé teszi a file-ok tartalmának titkosítását (Encrypting File System), amit csakis kizárólag a titkosítást elvégző operációs rendszer futása alatt, csak a titkosítást végző személy oldhat fel – no meg a rendszergazda (ez utóbbi kiskapu is becsukható). A file-ok adatterületét DES-algoritmussal lehet titkosítani, ez ugyan nem a világ legerősebb algoritmusa, de azért igencsak hosszú idő és fáradságos munka feltörni. Nem beszélve arról, hogy minden file-nak egyedi DES kulcsa van, azaz minden egyes file-on külön-külön el kellene végezni a feltörést – ebbe minden hacker beleőszül.



Kicsit esetlen megoldás, hogy a DES kulcsokat kódoló nyilvános kulcsú titkosítás kulcsai alapesetben a felhasználó profile-jába kerülnek, e gond megoldására a Microsoft a Smart Cardok használatát ajánlja.

További újdonság, hogy a WINNT és a SYSTEM32 rendszerkönyvtár végre nem Everyone-Full Control jogosultsággal „felvértezve" települ, hanem valóban csak a működéshez szükséges legszűkebb jogokkal, azaz a felhasználók csak olvashatják ezek tartalmát. Ennek a beállításnak voltak ugyan előzményei a Windows NT Service Pack 4-ben, de teljes körűvé csak most válhatott, hisz a felhasználói profilok könyvtárai végre kikerültek a WINNT alól (a gyökérkönyvtárban lévő *Documents and Settingsben* találhatók). Ezzel jó néhány korábbi file-átnevezési trükknek egyszer s mindenkorra befellegzett. Pedig az egyes rendszerfile-ok lecserélése micsoda fergeteges lehetőséget kínált akár egyszerű felhasználók számára is!

A rendszergazdai jogosultsághoz vezető egyik legkönnyebb utat bizony eltorlaszolták.

A regisztrációs adatbázis biztonsága

A regisztrációs adatbázis a Windows 2000-ben is fontos szerepet tölt be, bár a tartományvezérlők biztonsági adatbázisa már nem a SAM-ban (Security Access Manager) tárolódik, hanem az Active Directory file-jában, az NTDS.DIT-ben. (Ezzel az a szerencse, hogy egyelőre senki sem ismeri a belső felépítését, a szerencsétlenség pedig, hogy a gyengeségeit sem. Mindenesetre van bő két hónapunk, amíg a hackerek megbarátkoznak vele.) Mi maradt tehát a registryben? Minden egyéb beállítás, azaz a telepített alkalmazások, a szolgáltatások, az eszközök és a vezérlők, a COM összetevők, valamint a házirend (policy) stb. beállításai. A biztonság növelésének eredményeképpen a Windows 2000 ebben is újragondolt jogosultságrendszerrel bír, vagyis ebben is éppoly keveset tehetünk rendszergazdai jogosultság nélkül, mint a WINNT könyvtárban. (A korábbi NT verziókban ugyanis lehetett egyet s mást variálni...) Ne feledjük azonban, hogy a SAM biztonsági szerepe csak a tartományvezérlőkön szűnt meg, és ott is csak addig, amíg vissza nem minősítjük tagkiszolgálóvá a gépet, vagy hibaelhárítási okokból ki nem választunk olyan rendszerindítási üzemmódot (Safe Mode), amelyben az Active Directory nem indul el, s máris a SAM dolgozik. A SAM file védelme tehát továbbra is fontos, ebből ugyanis – ha nem is triviális módon – ki lehet szedni a felhasználók jelszavait, aminek veszélyességét nem kell magyaráznom. Honnan szerez a hacker SAM file-t? Amíg a Windows 2000 fut, addig innen nem lehet ellopni. De a kikapcsolt gépen kívül az Emergency Repair Disk és az operációs rendszerről készített szalagos mentés is remek lelőhely (ha már a főnök kívánságára muszáj menteni, akkor legalább zárjuk el a szalagot és az ERD lemezt mások elől).

További fontos adattartalom a regisztrációs adatbázisban a csoportos házirend (Group Policy), mellyel nemcsak a felhasználók életét megkeserítő tiltásokat, hanem igen fontos biztonsági szolgáltatásokat is be tudunk állítani. A Windows 2000, a Windows NT hagyománytartó utódaként rengeteg olyan biztonsági szolgáltatást tartalmaz, amelyek bekapcsolása a regisztrációs adatbázis különböző rejtett bugyraiba történő varázsbitek beírásával történik. Míg a szolgáltatások java része már a Windows NT különböző javítócsomagjaiban megjelent, gyakorlatilag senki sem használta ezeket, mert ugyan ki vállalta volna a vállalat ötszáz gépének (hibátlan!) beállítását, folyamatos ellenőrzését és karbantartását? A Service Pack 4 erre a feladatra már eléggé kiforrott eszközt (SecEdit) tartalmazott, de azt sem használta senki – pedig még a bitek helyét sem kellett ismerni, néhány ügyes egérkattintás elegendő lett volna. Most viszont a rendszergazdák orra előtt lesz a csoportos házirend, amellyel a security-varázsbitek központi helyről tetszőleges számú munkaállomáson állíthatók be. Magára vessen, aki továbbra sem használja ezeket. Miket is? Tekintsük át a lehetőségeket (nem a varázsbitekre gondolok, mert erről külön cikket lehetne írni). Hogy azért mégse kerüljem el teljesen ezt az óriási témakört, vegyünk két varázsbitet, amelyek hacker-ellenes hatása megkérdőjelezhetetlen.

SMB digitális aláírás, „The man in the middle" típusú támadás ellen:

Itt arról van szó, hogy a Windows 2000-es gépek minden elküldött SMB (Server Message Block) üzenetet nyílt kulcsú titkosítással látnak el, ennek publikus kulcsát azután az SMB csomaggal együtt küldik át a hálózaton. Ezzel a módszerrel az adatok ugyan továbbra is olvasható módon utaznak a hálózaton, de senki sem képes azokat meghamisítani, mert privát kulcs híján képtelen a módosítást észrevehetetlenné tenni. Az SMB digitális aláírás teljesítménycsökkentő hatása jelentős, hiszen minden csomagra le kell futtatni az algoritmust – 1 MB átküldése során mintegy ezerszer.

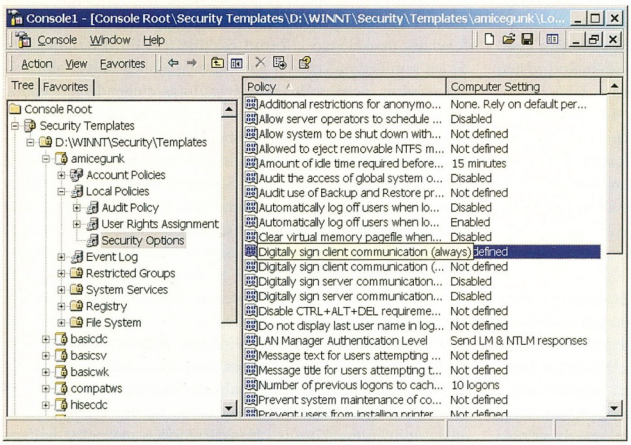
Lan Manager jelszóküldés tiltása: L0phtcrack és egyéb hálózati jelszólopók ellen. A windowsos bejelentkezések titkosított jelszavainak hálózatról történő „leemelése" nem bűn, inkább az a baj, hogy a titkosítási algoritmusok egyike (az IBM Lan Manager-féle) botrányosan gyenge. Egyirányú létére (hash) visszafelé is működik. Hálózati jelszólopás ellen az tűnik legegyszerűbbnek, ha ezt a fajta jelszótitkosítást kitiltjuk. Ez azonban kétélű fegyver: a Windows 98 és felmenői, a névadó Lan Manager és bizonyos öreg SAMBA kiszolgálók LanMan titkosítást használnak. Ezeknek búcsút kell(ene) mondanunk – és a kérdés máris politikai síkra terelődött.

Most pedig tekintsük át az elméletet.

Security Configuration Editor (SecEdit)

Az előző két varázsbit mindenkit meggyőzhetett arról, hogy nem lehet a vállalat összes gépén egységes beállításokat alkalmazni. Vagy a kívánatos teljesítmény elérésének szándéka, vagy a bevásárolt SAMBA Serverek, vagy valami más akadályozhatja meg a rendszergazdát abban, hogy a kitalált legerősebb biztonsággal telepítse összes gépet. Marad tehát a folto-

zás, egyfajta heterogén biztonsági „modell" megvalósítása. Ebben segít a SecEdit, mellyel biztonsági beállítás prototípusokat kísérletezhetünk ki, ezeket elmenthetjük, majd a vállalat megfelelő gépeire – a csoportos házirend segítségével – egyenruhaként ráhúzhatjuk. A Windows 2000 tartalmaz néhány – hogy a képzavar költői eszközével éljek – „konyhakész zubbonyt", ezek akár megfelelők lehetnek. Van SecureDC (biztonságos tartományvezérlő), HisecDC (roppant biztonságos tartományvezérlő), BasicWk (alap-munkaállomás) stb. zubbonyunk, ezekből lehet szükség esetén újat szabni. További remek lehetőség az elemzés, mellyel megállapítható, hogy valamelyik kiszemelt számítógép varázsbitjei megfelelnek-e mondjuk a HisecDC beállítás által megkövetelt rendnek. A *fenti ábrán* testre szabott, „amicégünk" névre hallgató beállítás látható, a jobb oldali panelen pedig az egér éppen az SMB aláírás bekapcsolásán gondolkodik.



A hálózati adatforgalom biztonsága

Foglalkozzunk egy kicsit a hálózati adatforgalom biztonságának kérdésével is. A tipikus vállalati hálózati technológiák (Ethernet, illetve itt-ott elvétve Token Ring) az úgynevezett üzenetszórásos hálózatok körébe tartoznak, azaz alapesetben minden egyes, az adott hálózaton „lógó" eszköz minden hálózati forgalomról értesül, de csak azokat a kereteket juttatja el az operációs rendszernek, amelyeknek a címe neki megfelelő (unicast, multicast, broadcast).

A hálózati kártyák többségét azonban át lehet kapcsolni úgynevezett promiscuous (fűvel-fával) üzemmódba, melyben minden egyes keretet válogatás nélkül továbbít az operációs rendszernek, azaz sniffel. Megfelelő programmal a sniffelt hálózati forgalomból ki lehet mazsolázni a legértékesebb adatokat, illetve jelszavakat vagy dokumentumokat stb. A sniffelők ellen sokféle módon lehet védekezni, ezek közül az üzenetszórásos modell kiküszöbölése a legkézenfekvőbb. Ethernet hálózatokban ezt switchekkel lehet megvalósítani, amelyek csakis kizárólag azokhoz a hálózati eszközökhöz juttatják el a forgalmat, ahová az igyekszik.

Ha switch beszerzésére nincs mód, el kell gondolkodnunk a hálózati forgalom titkosításán, amire a Windows 2000 többféle megoldást is kínál. Lehetőség van úgynevezett virtuális magánhálózati (Virtual Private Network, VPN) alagutak kialakítására (PPTP és L2TP protokollokkal), illetve az IP-forgalom közvetlen titkosítására IPSec technológiával. Mindkét modellnek vannak előnyei és hátrányai. Az alagutak olyan esetben is lehetővé teszik az adatátvitelt, amikor esetleg még a route-olás feltételei sincsenek meg (például IPX-szegmensek összekötése Interneten), viszont a kettős protokollfejléc és az újracsomagolás miatt valószínű, hogy a csomagok nem fognak elférni ugyanabban a keretben, mint a titkosítás előtt, így töredezetté válhatnak. Az IPSec használatának pedig az az óriási előnye, hogy minden Windows 2000 gépen, azaz végponttól végpontig használható. Sőt, az alkalmazás feltételeit központilag, csoportos házirenddel lehet beállítani. Mindkét technológia egyenértékűen használható a hálózati forgalom (emberi időszámításon belüli) visszafejthetetlen titkosítására.

A bejelentkezés hálózati forgalmának biztonsága

Olyan hálózatokban, melyekben lemondunk a Microsoft korábbi operációs rendszereivel való kompatibilitásról, teljesen el lehet szakadni nemcsak a tökéletesen visszafejthető LanMan, hanem a semmivel és senkivel sem kompatibilis NTLM Challenge/Response bejelentkezési algoritmustól is, és át lehet térni az Internet-szabvány Kerberos bejelentkezésre. Ennek a rendszernek a működése arra hasonlít, ahogyan az osztrák-magyar határon kisétálunk: felmutatjuk a mindkét fél számára elfogadott hatóság (BM) által kiállított okmányt. Ezt a jogosultság-ellenőrző kiskatona elfogadja, és nem rohan be a budapesti központba az okmány ellenőrzésére.

A Kerberos rendszerben az okmány neve: jegy (ticket). Hogyan véd ez a hackerek ellen? Nos, ez a modell önmagában nem véd, csak a jelszavak és megfelelő kulcsok hatékony titkosítása segít. A Kerberos azonban itt is megállja a helyét.

Amennyiben ez a néhány oldal felkeltette kíváncsiságukat, a következő témakörök áll(hat)nak még előttünk: részletekbe menő Kerberos, Certificate Server és Smart Card útmutató.

Biztonságos honlap Certificate Serverrel

Borbély András
aborbely@protomix.hu

Nem is olyan régen az Internet még a kutatóintézetek, egyetemek hálózata volt, és az adatforgalom jelentős részét nyilvános kiadványok, illetve cikkek tették ki. Mára a kereskedelmi használat egyre inkább túlsúlyba kerül, melyben a továbbított információk java része bizalmas. Ennek köszönhetően megnőtt a titkosítás és hitelesítés iránti igény.

A megbízható, kényelmesen használható titkosító és hitelesítő megoldások kifejlesztése a szükségesnél talán hosszabb időt vett igénybe, ugyanis az Internet kialakulásakor nem fektettek hangsúlyt erre a kérdésre, ezért a protokollok nem tartalmazták a megfelelő kiskapukat a kódolás beépítésére.

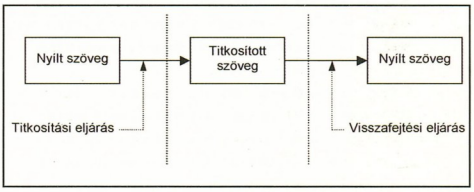
Írásunkban egyrészt áttekintjük, hogy a nyilvános kulcsú titkosítás hogyan alakult ki, másrészt a Windows 2000 platformon működő Internet Information Server példáján keresztül bemutatjuk a Microsoft Certificate Server felhasználási lehetőségeit.

Rejtjelezés

Először vizsgáljuk meg, hogy a tikosításnak milyen elvi háttere van, miféle megoldások alakultak ki, és ezek közül melyikeket használják jelenleg leggyakrabban.

Elvi folyamat

Vázlatszinten a titkosítási folyamat igen egyszerű. Az olvasható (szaknyelven nyílt vagy plain) szöveget először a titkosítási kulcs (encryption key) segítségével titkos, kívülállók számára olvashatatlan (ciphertext) szöveggé alakítjuk. (Érdekességképpen: a „cipher" szó a szanszkrit „sunyam" – üres szóból ered.)



A titkosítási folyamat vázlata

Ezt elküldjük a megfelelő személynek, aki a megfejtési kulcs (decryption key) segítségével ismét nyílt szöveggé fejti vissza.

Milyen alapvető elvárásokat támaszthatunk a fenti módszer iránt?

- A titkosított szöveget illetéktelen személy ne fejthesse vissza,
- megbízhatóan megismerjük, kivel váltunk üzenetet,
- az üzenet küldője ne tudja letagadni, hogy ő indította útjára az üzenetet.

Ezen kívül a modern titkosítási eljárásokkal szemben alapvető feltétel, hogy akkor is erős védelmet nyújtsanak, ha a betörő ismeri az alkalmazott eljárást, de nem ismeri a pillanatnyi kulcsot. Sajnos, a piacon még ma is több olyan megoldás található, amely a kódoló algoritmus titkosságán alapul, és mikor ez napvilágra kerül, használhatatlanná válik (például GSM telefonok, DVD filmlemezek stb.).

Az egyik legfontosabb szabály a kódolás kiválasztásakor, hogy a titkosított adatok megfejtési költsége sokkal nagyobb legyen az adatok értékénél!

Tekintsük át, milyen megoldások léteznek, ezeket hogyan

alkalmazhatjuk internetes környezetben, és ezt hogy alakíthatjuk ki könnyen és megbízhatóan a Microsoft Certificate Server segítségével.

Történelmi előzmények

Már az időszámításunk előtti korban felmerült az igény, hogy el lehessen rejteni a leírt szövegeket az avatatlanok elől. *Aineiasz Taktikosz* i.e. 360 körül írt Poliorkétika könyvében már több tucat olyan titkosírási módszert sorol fel, melyek betű kihagyáson és számokkal vagy pontokkal való helyettesítésen alapulnak.

Julius Caesar a betűhelyettesítés módszerét alkalmazta a galliai hadjárata idején. Az A betűt például D-re, a B betűt E-re cserélte, vagyis az ábécében 3 betűvel eltolta a nyílt szöveget. Az ehhez hasonló kódolást próbálkozással meglehetősen gyorsan és egyszerűen meg lehet fejteni. Egyszerűen végig kell nézni – angol ábécé szerint – a 26-féle betűeltolást, és ki kell választani a megfelelőt.

A reneszánsz idején *Johannes Heidenburg* jezsuita práter 1518-ban megjelent könyvében az alkimista tikos jelölések leírása között olvashatjuk a „transzpozíciós tabella" (felcserélési táblázat) módszerét, mely a modern betű-behelyettesítéses rejtjelezés őse. A nyílt szöveget szakaszosan, más és más számmal jelölt kulccsal rejtjelezte.

E módszer már jóval megbízhatóbb, hiszen 26!-féle betűhelyettesítés-permutáció lehetséges. Mégis aránylag könnyen feltörhető, mivel az értelmes szövegekben az egyes betűk aránya nem azonos (például a legtöbb nyugati nyelvben az „e" a leggyakoribb hang). A visszafejtéshez tehát mindössze meg kell nézni, melyik betűk milyen gyakorisággal fordulnak elő, és ez alapján kideríthető, hogy mit helyettesítenek (váltogatott kódkészlet esetén azonban először ki kell találni, hogy a kód hogyan változik).

A francia *Blaise de Vigenère* sikeresen továbbfejlesztette ezt az eljárást. Az övé az első ismert módszer, amely szöveges kulcsot használ. Sőt, a kulcs még az eljárás ismeretében is meglehetősen nehezen visszafejthető. Vigenère e titkosítást megfejthetetlennek nevezte, és tény, hogy csak századokkal később, 1863-ban sikerült a megfejtésére módszert kidolgozni.

A módszer lényege, hogy először annyiszor a nyílt szöveg alá kell írni a kulcsot, hogy a szöveg minden betűje alá jusson kulcsbetű, majd pedig a szöveg egyes betűit egy táblázat használatával attól függően kell eltolni az ábécében, hogy a kulcs melyik betűje található alattuk.

A világtörténelemmel párhuzamosan a magyar történelemben is rábukkanhatunk a titkosírás alkalmazására. *I. Ferdinánd* magyar király (1503–1564) és német-római császár által használt eljárásban a rejtjeleket különleges alakú jelekből képezték, és a nyílt latin ábécét is módosították. Összevonták az E, CE és U, V betűket, és tudatosan kihagyták a K és Z betűt. Később *Balassi Bálint*, majd *Rákóczi Ferenc*, *Pázmány Péter* és *Zrínyi Miklós* is használt illetve írt teljesen vagy részben, rejtjelezett levelet.

A titkosítás bonyolultságának növekedésével megjelentek a rejtjelező gépek is, melyek igyekeztek egyszerűbbé tenni a nagyrészt gépies folyamatot. Az 1800 évek elején széles körűen elterjedt a tárcsás rejtjelező gép, melyben több kevert ábécés tárcsát alkalmaztak. Az ilyen módon rejtjelezett szöveg megfejtésének ideje nagyjából 6 óra és három nap között mozgott, ezért a kulcsszót előre kidolgozott módszer szerint 6 óránként megváltoztatták.

1926-ben a német hadsereg bevezette az *Anton Scherbius* által készített Enigma rejtjelező gépet. E masina azóta legendává vált, hiszen használata és a kódok megfejtése komoly szerepet játszott a második világháború történetében.

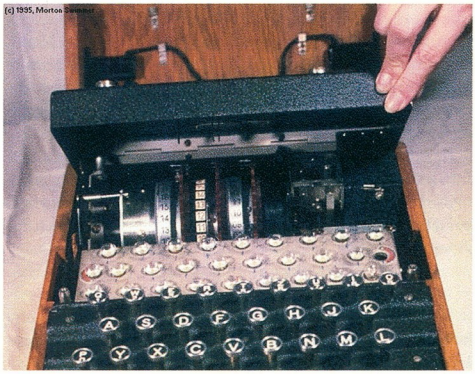
Az Enigma is betűhelyettesítést alkalmazott, viszont minden egyes betű után váltotta a helyettesítő táblázatot. E hatást három „helyettesítő tárcsával" érte el, amelyek az autók kilométer-számlálójához hasonlóan forogtak. A betűfrekvenciák figyelését közvetlenül nem lehetett felhasználni az Enigma fel-

Így fest az egyszerű helyettesítéses kódoláshoz használt táblázat

Eredeti betű	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
Kódbetű	**E**	**Z**	**A**	**K**	**O**	**D**	**X**	**W**	**B**	**J**	**L**	**Q**	**U**
Eredeti betű	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
Kódbetű	**Y**	**T**	**I**	**P**	**R**	**M**	**H**	**C**	**F**	**S**	**V**	**G**	**N**

A titkosításhoz a szöveg betűit egyenként le kell cserélni:

Ez itt egy példa a kódolt szövegre
On bhh oxg ioqkc e ltktqh mntfoxre



törésére, mivel a kódváltogatás teljesen összekeverte az ábécét. Ráadásul ugyanaz a helyettesítő táblázat szinte sose fordult elő kétszer, ugyanis a gép tizenhétezer betű után tért vissza ugyanarra a pontra.

Mivel a kódolt szöveg nemcsak a tárcsák drótozásától, hanem sorrendjüktől és a kiinduló helyzettől is függött, a gép optimális esetben nagyon erős biztonságot nyújtott.

Az Enigma igen sok fejtörést és eredménytelen kísérletet okozott az angol haditengerészet számára. Bár a lengyelek már 1928-ban hozzájutottak az egyik korai modellhez, és ez alapján komoly előrelépéseket tettek a feltörő eljárások kidolgozásában, megbízható módszert azonban csak azután sikerült kidolgozni, hogy 1941 tavaszán megszerezték az egyik német tengeralattjáró két tökéletlenül megsemmisített rejtjelező gépét és néhány kódkönyvét.

Ezekkel a kiegészítő ismeretekkel felfegyverkezve, valamint a németek lustaságát és fegyelmezetlenségét kihasználva az *Alan Turing* által vezetett csapatnak már csak új gépre (az inverz Enigmának tekinthető „Bombe"-ra) volt szüksége, és máris sikeresen hozzájutottak a német üzenetek tartalmához. Amennyiben az ellenfél ügyelt volna arra, hogy a titkos üzenetekben ne forduljanak elő sejthető szavak (pl.: időjárás-jelentések, „an general..."-lal kezdődő üzenetek stb.), és rendszeresen váltogatták volna a kódoló tárcsákat, talán a történelem kerekei is másképpen forogtak volna.

A hidegháború alatt a titkosítás tudománya természetesen nagymértékben fejlődött. Az igazi áttörést azonban mégiscsak a számítógépek alkalmazása hozta.

Az Egyesült Államok kormányának 1976 decemberében elfogadott szabványa DES (Data Encryption Standard) néven vált ismertté. Az eljárás 56 bites kulcs segítségével 64 bites tömböket titkosít 64 bites tömbökké a bitek többlépcsős, rafinált cserélgetésével. Már 1977-ben felvetődött a lehetősége, hogy megfelelő hardverteljesítmény esetén a tikosított szöveg nyers próbálgatással visszafejthető, 1993-ban pedig *Biham és Shamir* kidolgozott a próbálgatásnál hatékonyabb visszafejtési eljárást is.

A DES-algoritmus, sajnos eléggé merevre sikeredett, ugyanis nem lehet egyszerűen megnövelni az alkalmazott kulcshosszúságot. Mivel az 56 bites változat mára már ésszerű befektetéssel napok alatt feltörhető, átmeneti megoldásként a többszörös alkalmazást (Double DES és Triple DES) javasolták (a 3DES 156 bites kulccsal körülbelül 112 bites erősséget ad). Időközben azonban rugalmasabb helyettesítő megoldások is születtek, mint például az IDEA (Ideal Data Encryption Algorithm), a Blowfish, a CAST vagy az RC5. Ezek mindegyike képes 128 bites kulcsot (is) használni, ez azt jelenti, hogy a primitív próbálkozás módszerét alkalmazó támadónak 2^128 kulcsot kell végigpróbálnia, ami éppen 2^64-szer annyi, mint a 64 bites kódolás esetén. A fent említett négy algoritmus egyébként már szinte biztosan „erősnek" tekinthető, azaz nincs a próbálgatásnál hatékonyabb módszer megfejtésükre (ellenpéldaként álljon itt a DVD-k esetében alkalmazott, eredetileg is nagyon gyenge, mindössze 40 bites kulcsokat használó CSS kódolás, amelyet 26 bitnyi ügyesen megválasztott variáció végigpróbálgatásával fel lehet törni). A „szinte" kitétel arra vonatkozik, hogy a feltörhetetlenségre matematikai bizonyítás nincs, viszont évek hosszú során át rengeteg erre irányuló szakértői kísérlet megbukott.

A mai számítási teljesítmények mellett a legalább 64 bites kulcsok tekinthetők biztonságosnak, ezek feltöréséhez még komolyabb felszereltség birtokában is néhány év szükséges. Aki biztosra akar menni, az 128 bites kulcsot alkalmaz, amely – a fejlesztés igencsak kezdeti állapotában lévő kvantum-számítógépek híján – pár száz éven belül aligha fejthető meg.

A DES formális, kormányszintű helyettesítésére 1997 szeptemberében pályázatot hirdettek. Valószínűleg hamarosan meg fog születni az új szabvány AES (Advanced Encryption Standard) néven (128 bites blokkhosszal és 128, 196 valamint 256 bites kulcshosszal).

Nyilvános kulcsú titkosítás elve

A fenti példák mindegyikében a titkosítási és a megfejtési kulcs azonos, vagyis szimmetrikus kódolásról beszélhetünk. Ez felveti azt a kérdést, hogy a kulcsban az üzenet küldőjének és vevőjének meg kell állapodnia, ráadásul erre a célra rendszerint ugyanaz a nem biztonságos csatorna áll rendelkezésükre, mint a további kommunikációra. Emellett mindkét félnek meg kell bíznia egymásban, hogy a kulcsot kellő gondossággal őrzik, a gyanús kulcsot pedig rendszeresen újra kell cserélni.

1976-ban *Whitfield Diffie* és *Martin Hellman* másik elvből indult ki. Olyan eljárást dolgoztak ki, amelyben a titkosítási és megfejtési kulcs különbözik egymástól. A titkosítási kulcsból nem lehet a megfejtési kulcsra következtetni (és vice versa), így elegendő csak ez utóbbit titokban tartani (private key), a titkosítási kulcsot bárki számára elérhetővé tehetjük (public key). Az összetartozó kulcspár kiötléséért egy véletlengenerátort használó algoritmus felelős. Mivel nagyon hosszú kulcsokról van szó, asztronomikusan kicsi az esélye, hogy két embernek ugyanaz a kulcspár pottyanjon ki (ez később, az aláírások esetében fontos).

A két félnek így nem kell feltétlenül ismernie egymást, mégis biztonságosan üzenetet cserélhet nem megbízható csatornán keresztül is. Hiába hallgatja le bármely rosszindulatú személy a kettejük között folyó beszélgetést, ebből mindössze azt tudhatja meg, hogy mi a két fél nyilvános kulcsa, amihez viszont aligha kell hallgatóznia, hiszen esetleg az illetők weblapján is megtalálhatja azt.

A *Rivest*, *Shamir* és *Adleman* által kifejlesztett RSA-algoritmus az egyik legelterjedtebb nyilvános kulcsú titkosítási módszer. Matematikai alapja az a tény, hogy két prímszámot villámgyorsan össze lehet szorozni, annak kiderítése azonban, hogy adott összetett szám mely két (vagy több) prímszám szorzata, mindössze (a szám hosszával csaknem exponenciálisan

növekvő mennyiségű) próbálgatással, borzasztó lassan lehetséges. A gyakorlatban ezen algoritmus esetében 2048 bites, vagy ennél hosszabb kulcsokat érdemes használni.

Alkalmazási lehetőségek

A titkosítás és a digitális aláírás a nyilvános kulcsú rejtjelezés két legfontosabb felhasználási területe. Mivel e két alkalmazás más-más igényeket támaszt, ezért célszerű személyenként két kulcspárt használni, egyet rejtjelezésre (exchange key), egyet pedig aláírásra (signature key).

Az elektronikus dokumentumon a digitális aláírás ugyanazt a szerepet tölti be, mint a papíron a saját kezű aláírásunk: jogi értelemben is hitelesen bizonyítja, hogy a dokumentum tőlünk származik. Ezért az egyik igen fontos követelmény, hogy az aláírásra használt kulcsunkhoz más személy semmiképpen ne juthasson hozzá. A másik fontos feltétel, hogy adott dokumentumhoz tartozó aláírást ne lehessen átmásolni másik dokumentumra. Ezért az aláírás képzésekor felhasználják a dokumentum tartalmát is.

A gyakorlatban a digitális aláírás egy számsor (ez sokszor külön file-ban található a dokumentum mellett). Készítésének első lépése, hogy az aláírandó dokumentumból „párlatot" készítünk egyirányú, úgynevezett hash-függvénnyel. E függvény olyan – a dokumentum méreténél sokkal kisebb – számot generál, amely a dokumentum minden egyes bitjétől függ, a legkisebb változás is másik hash-értéket hoz létre. Ugyancsak fontos, hogy nincs ésszerű ideig futó módszer arra, hogy adott hash-értékhez megfelelő dokumentumot gyártsunk (ami ráadásul még értelmes is), így teljesen kizárt, hogy az aláírás másik dokumentumhoz használható legyen.

Utolsó lépésként a párlatot a pillanatnyi keltezéssel és egyéb fontos információkkal együtt titkosítani kell rejtett kulcsunkkal.

A kulcs titokban tartására jó megoldás a Smart Card használata. Ez azt jelenti, hogy olyan intelligens kártyánk van, amely hozzáférhetetlenül tárolja a titkos kulcsot, a betáplált dokumentumhoz pedig aláírást (lásd még a Smart Cardokról szóló *Hitelesség 2000 után Smart Card alkalmazásával* című cikkünket) ad ki.

A titkosításra használt kulccsal egy kicsit más a helyzet, hiszen ez nem azonosításra, hanem a nyílt szöveg elrejtésére szolgál. Vállalati környezetben gyakran megkövetelt igény, hogy a munkatársak által kódolt dokumentumok az arra illetékes személyek – például a cég legfelsőbb vezetése – által visszafejthetők legyenek.

Vagyis a kulcs elvesztése esetén a dokumentumok tartalma ne vesszen el, ezért ezekről a kulcsokról gyakran – szigorú biztonsági intézkedések mellett – másolatot őriznek. Ezek segítségével indokolt, vitás esetben az okmányok eredeti szövege megkapható. A felhasználási területtől függetlenül a kulcsok kiosztása is fontos feladat. A kulcs tartalmaz olyan személyes adatokat, mint a családi-, és a keresztnév, az e-mailcím, a telefonszám vagy a beosztás stb. Ezeket általában nem maga a kulcs gazdája adja meg, hanem a meglévő vállalatirányítási, levelezési vagy személyi rendszerek szolgáltatják. Ez egyrészt megteremti az adatok hitelességét, másrészt megkönnyíti a kulcs hatékony előállítását.

Gyakorlat

Egy konkrét példa kapcsán tekintsük át, hogyan néz ki a gyakorlatban a biztonságos üzenetváltás nyilvános kulcsú tikosítás felhasználásával.

Tételezzük fel, hogy *Éva* és *Ádám* egy bizonyos esemény óta távol élnek egymástól, de naponta szeretnének üzenetet váltani oly módon, hogy ezt illetéktelen harmadik személy, például *Lucifer* ne tudja elolvasni.

Amikor Ádám levelet akar küldeni Évának, először beszerzi Éva nyilvános kulcsát, majd ezt használva rejtjelezi a levelet. Mikor Éva megkapja az üzenetet, megoldja saját titkos kulcsával, mivel ez a kulcs az Ádám által használt nyilvános kulcs pontos párja. Lucifer nem ismerheti a titkos kulcsot, így nem is fejtheti vissza a kódolt üzenetet.

Aláírás

Elképzelhető, hogy Lucifer nem akar hallgatózni, csupán hamis információkat szeretne adni Évának. Mivel Éva nyilvános kulcsa számára is hozzáférhető, könnyen üzenhet Ádám nevében – akár titkosan, akár nyíltan. Hogyan tudja hát Ádám igazolni, hogy ő írta a levelet? Mi sem egyszerűbb, digitális aláírást kell használnia.

Mindössze annyi a dolga, hogy fordítva használja a kulcsokat, a saját titkos kulcsát használja kódolásra. Ha Évának sikerül Ádám nyilvános kulcsával visszafejteni a levelet, biztosan tudhatja, hogy az nem hamisítvány.

Hitelesítés

A fenti megoldás még nem oszlatja el teljesen Éva aggodalmát a felől, hogy a levelet esetleg Lucifer küldte, hiszen csak arról győződhetett meg, hogy a kapott levél írójának birtokában van az általa Ádáménak hitt nyilvános kulcs párja. De hogy ez valóban Ádám kulcsa-e, azt nem tudhatja, az is lehet, hogy Lucifer álcázott kulcsáról van szó. Ez a bizonytalanság legegyszerűbben úgy küszöbölhető ki, ha a kulcscsere idejére a két fél találkozni tud, ami azonban nem mindig megoldható.

Ekkor olyan feddhetetlen negyedik szereplőnek, például *Madách Imrének* kell igazolnia a kulcsok származását, aki mindkét féllel találkozni tud.

Mikor Évánál jár, átadja saját nyilvános kulcsát, majd pedig készít egy aláírást, ami bizonyítja, hogy Éva nyilvános kulcsa ellenőrzötten hozzá tartozik. Ezután Ádámhoz látogat, és nála is megteszi ugyanezt. Most már nincs más dolga Ádámnak, mint elküldeni Éva számára az aláírt nyilvános kulcsát, amiről Éva Madách nyilvános kulcsának birtokában bizonyosan tudhatja, hogy eredeti.

Visszavonás

Ha az ifjú pár még egy kicsit óvatosabb, arról is gondoskodhat, hogy az se okozzon galibát, ha Lucifer fondorlatos módon hozzájut Éva titkos kulcsához. Ádámnak csak annyi a teendője, hogy mielőtt levelet küldene Évának, vagy amikor aláírt üzenetet kap tőle, a nyílt csatornán megkérdezi Madách Imrét, hogy titkos-e még Éva kulcsa. Az aláírt válasz hitelességét ellenőrizni tudja, hiszen találkozásuk során megkapta Madáchtól annak nyilvános kulcsát. Ha Éva titkos kulcsa nyilvánosságra kerül, azonnal jelzi ezt Madáchnak, aki legközelebb már a kiábrándító választ – vagy Éva új nyilvános kulcsát küldi vissza Ádámnak.

Microsoft Certificate Services

A fenti példán keresztül láthattuk, hogy a biztonságos adatforgalom hogyan kivitelezhető. Most tekintsük át, a Windows 2000 környezet milyen támogatást ad a nyilvános kulcsú titkosítás használatához.

Alapok

Akár szimmetrikus kulcsú, akár nyilvános kulcsú titkosításról vagy digitális aláírásról van szó, a Windows-platform termékei a CryptoAPI eljárásgyűjteményre támaszkodnak. Ez egyrészt könnyen használható, egységes felülettel elérhetővé tesz számos rejtjelezési algoritmust, másrészt pedig segítséget ad a kulcskészítés, a hitelesítés és a tárolás lépéseihez. A tényleges kódoló egységek, a CSP-k (cryptography service provider) szabadon váltogathatók az API mögött.

Kulcspár készítés

A kulcspár előállítása nem ördöngös feladat, többfajta beépített algoritmus (GemSAFE, RSA, DSS (Digital Signature Standard), DH (Diffie-Hellman)) közül válogathatunk, de a Microsoft CryptoAPI felület segítségével mód van más cégek által készített eljárás beillesztésére is.

Eldönthetjük azt is, hogy engedjük-e exportálni a kulcspár titkos tagját, vagyis a kulcspár gazdája továbbadhatja-e más személy számára a létrehozott titkos kulcsot.

A gyakorlati használat során általában a kulcspárok előállítását is a hitelesítő hatóság végzi, ez nagymértékben leegyszerűsíti a feladataink kivitelezését.

Hitelesítési kérelem és kiadása

Ahhoz, hogy nyilvános kulcsunkat hitelesítsük, először egy űrlapot kell kitöltenünk, melyen olyan személyes adatokon kívül, mint a név, az e-mail vagy telefon, fel kell tüntetnünk, mire akarjuk felhasználni a hitelesítést. A kitöltött űrlap alapján szabványos PKCS-7 dokumentum (certificate request) jön létre, ennek segítségével a Certificate Server a megfelelő hitelesítést kiadhatja, szintén szabványos PKCS-7 formátumban. Ez tartalmazza, hogy a hitelesítés mire terjedt ki.

Az PKCS-7 és PKCS-10 dokumentumok előállítására, illetve kezelésére „Enrollment" ActiveX Control is elérhető, ezt beépíthetjük a saját alkalmazásunkba, vagy feltehetjük a weblapunkra.

Lehet sablonokat (certificate request templates) is használni, ezek egyrészt mentesítik a felhasználót az űrlap kitöltésétől, másrészt szabályozzák, hogy ki milyen hitelesítést kérhet.

Hitelesítési kérés megismétlése

Ha a hitelesítést kérő felhasználó adatai nem változtak, csupán a hitelesítés járt le, nem kell új kulcspárt generálni, és így a folyamat sokkal egyszerűbb.

Visszavonás

Néhány esetben szükség lehet a hitelesítés visszavonására:

- a titkos kulcs elveszett, vagy vélhetően illetéktelen személy kezébe került;
- a hitelesítéshez csalással jutottak hozzá;
- a hitelesített kulcs valamely tulajdonsága érvényét vesztette (például a tulajdonosa munkahelyet váltott; – ez esetben nem lenne célszerű, ha a régi cég nevében írna alá).

A Certificate Server a visszavont hitelesítéseket a Certificate Revocation listába (CRL) gyűjti, ebből bárki megtudhatja, melyek az érvénytelen kulcsok (általában lejáratukig érdemes a listában tartani a visszavont hitelesítéseket).

Hitelesítési hierarchia

A hitelesítés tulajdonképpen nem más, mint digitális aláírás a hitelesítő hatóság (Certificate Authority – CA) részéről.

A gyanakvóbb olvasó nyilván feltette magában a kérdést: honnan lehet tudni, hogy a hitelesítő hatóság nyilvános kulcsa hiteles-e? Valóban, a hitelesítő hatóság nyilvános kulcsának érvényességét egy másik hatóság igazolja.

A hitelesítő szerverek ily módon rangsorba szervezhetők. A rangsor tetején a „Root Certificate Authority" áll, mely saját magát hitelesíti.

Intraneteknél az önhitelesítésnek nyilván nincs olyan jelentősége, ez esetben nyugodtan kiépíthetünk egy „szigetet", azaz a Certificate Servert root-CA módban telepíthetjük.

Mi az új a Certificate Serverben?

Maga a szervertermék NT 4.0-ra is elkészült. Lássuk, melyek azok a képességei, amelyek csak Windows 2000 alatt teljesednek ki igazán!

- Az új CryptoAPI eljárásgyűjtemény, mely kibővült a Public-Key Cryptography Standards (PKCS) formátumú dokumentumok kezelésével és a kulcsok tárolási helyeinek (certificate store) használatával.
- A hitelesítések kiadását és visszavonását segítő adminisztrációs modul.
- Több lehetőséget teremtő webes felület a hitelesítési kérések elkészítésére és azok telepítésére.

- Hardveralapú titkosítás (pl.: Smart Card) támogatása.
- Integráció a Windows 2000 Active Directoryjával.
- Hitelesítésre, kulcshasználatra vonatkozó házirendek összeállítása.
- Együttműködés nem Windows-alapú böngészőkkel és webszerverekkel.

Biztonságos honlap

A felsorolt lehetőségek tükrében tekintsük át, hogyan alakíthatunk ki olyan honlapot, mely biztonságos üzenetváltást nyújt az Interneten.

Az alább ismertetett példa szerveroldalon Internet Information Servert feltételez Windows 2000 platformon, míg kliensoldalon az Internet Explorer 5 használatát mutatja be. Feltételezzük továbbá, hogy a Certificate Servert root-CA beállítással telepítettük fel.

Mint azt az előző fejezetben láttuk, a kulcspár készítését és hitelesítését szintén a Certificate Server végzi.

Általában mind szerver-, mind kliensoldalon az alábbi lépéseket kell végrehajtanunk:

1. a hitelesítési kérelem elkészítése a Certificate Server számára;

2. a Certificate Serverrel a kérelem elfogadtatása, és a hitelesítés kibocsáttatása;

3. a kibocsátott hitelesítés hozzárendelése a webszerverhez vagy a böngészőhöz.

4. SSL-konfigurálás.

Szerver

Indítsuk el a webszerver *Control Panel/Administrative Tools/Internet Services Manager* modulját, a biztonsági beállítások részben válasszuk a *Secure Communication/Server Certificate* menüpontot.

A *Create new certificate* lehetőséget kiválasztva először készítsük el a hitelesítési kérelmet. Figyeljünk arra, hogy a szerver nevének (common name) a DNS-bejegyzésben szereplő szervernevet, és ne a NetBIOS nevet adjuk meg!

Az így elkészített szöveges formátumú file-t oda kell adnunk a Certificate Servernek, hogy ez alapján elkészítse a hitelesítést. Ehhez a Certificate Server webfelületét kell felhasználnunk. A *Request a certificate/Advanced request/Submit a certificate request using a base64 encoded PKCS #10 file* opciók kiválasztása után a hitelesítési kérelmet egyszerűen másoljuk bele a megjelenő mezőbe. A hitelesítési kérelmünk elfogadásra vár.

2. A *Control Panel/Administrative Tools/Certification Authority* adminisztrációs moduljában lévő *Pending Request* mappában keressük meg az általunk kért hitelesítéshez tartozó bejegyzést. Az „issue" lépés segítségével adjuk ki a hitelesítést.

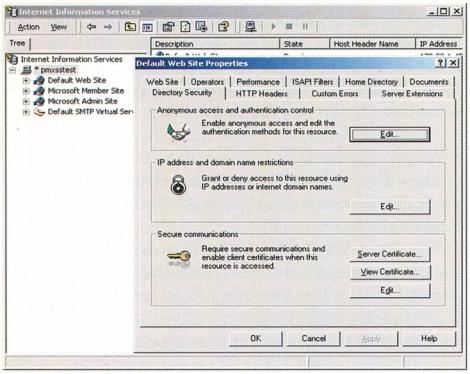
Térjünk most vissza a weboldalakhoz, hogy a kiadott hitelesítést hozzá tudjuk illeszteni a webszerverhez. Ehhez a *Check on a pending certificate* menü után válasszuk ki a kérelmünket, és töltsük le a kulcsunkat.

3. Válasszuk ki ismét az *Internet Services Manager* modul *Server Certificate* menüpontját. Most már kiválaszthatjuk az *Install certificate* opciót, és az előző lépésben letöltött file-t megadva befejezhetjük a hitelesítési lépéseket.

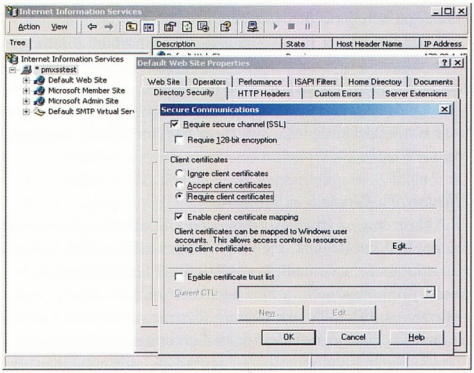
4. A Secure Communications részben az Edit menüpont most már megjelenik. Ebben követeljük meg az SSL-használatot és a klienshitelesítést.

Kliens

1. Használjuk ismét a Certificate Server webfelületét! A *Request a certificate/User certificate Request* menüpontban ügyeljünk arra, hogy *Browser* tanúsítványt kérünk.



A webszerver már rendelkezik kulcssal: használhatjuk az Edit gombot

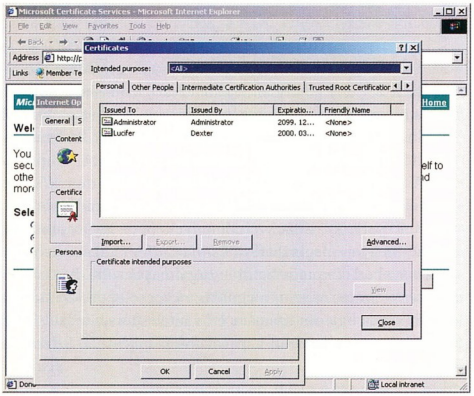


Követeljük meg a kliensektől az SSL-t és a hitelesítést

2. Állítsuk ki a hitelesítést a webszerverhez hasonlóan a *Certification Authority* adminisztrációs modul segítségével.

3. Térjünk vissza a Certificate Server HTML-oldalához, és a *Check on a pending certificate* menü után a kérelmünket kiválasztva feltelepíthetjük a hiteles kulcspárt az *Install this certificate* link kiválasztásával.

A sikeres telepítést ellenőrizhetjük a böngészőn a *Tools /Internet options.../Content/Certificates...* opciók kiválasztásával. Ekkor ugyanis az új bejegyzésnek meg kell jelennie a személyes tanúsítványok listájában.



A böngészőben láthatjuk a telepített hitelesítéseket

Certificate Server hitelesítése

Még egy apró dolgot kell megtennünk. Böngészőnk számára át kell adni a Certificate Server nyilvános kulcsát és ennek tanúsítványát. Ez általában a Certificate Server telepítése során megadott paraméterek alapján jön létre, és alapértelmezésben a \CertAdmin könyvtárban található. A .CER kiterjesztésű file a gép nevét is tartalmazza.

Figyeljünk arra, hogy a hitelesítés „telepítése" során *certification store* paraméternek a *Trusted Root Certification Authorities\Local Computer* értéket adjuk meg.

Kulcs–felhasználó összerendelés

A szerver a kulcsunk alapján képes adott felhasználói azonosítóhoz, vagyis adott NT-userhez rendelni bennünket. Erre azért lehet szükség, mert általában file-rendszer szinten, vagyis az NTFS beállítások között a weboldalak hozzáférése is korlátozott.

Ezt a hozzárendelést a *Secure Communications* menüpont *Enable client certification mapping* pontjában állíthatjuk be. Válasszunk tehát itt olyan NT-felhasználót, akinek joga van file-rendszer szinten hozzáférni a HTML-oldalhoz.

Használat

Ha most a szerverünkre nem a http://server néven, hanem https://server néven hivatkozunk, akkor már a biztonságos csatornát használjuk.

A szerver elérése során a böngészőnknek fel kell ajánlania, hogy melyik kulccsal szeretnénk elérni, ezt kiválasztva megtekinthetjük a weboldalakat.

Tanácsok, tippek

Végül néhány tanács a gyakorlati használathoz.

- Bánjunk kellő körültekintéssel a kulccsal a tárolás során, mert az egész titkosítás semmit sem ér, ha a kulcs idegen kezekbe kerül. Ezért ne hagyjuk a merevlemezen, a weboldalak között vagy levélben.
- A kulcsokra alkalmazhatjuk a many to one összerendelést, ez esetben több kulcsot rendelünk egyetlen Windows NT felhasználóhoz.
- Az SSL-csatornát és az NTLM-authentikációt egyszerre is használhatjuk adott honlap elérésére.
- A kulcsokat személyre szólóan és ne tevékenységhez kapcsolva osszuk ki.
- A lehető legnagyobb biztonság és hitelesség érdekében feltétlenül célszerű feltenni a kliensekre és a szerverekre az év eleje óta már hazánkból is letölthető Windows 2000 és az Internet Explorer High Encryption Packet (a webcímeket lásd a mutatók felsorolásában).

Mutatók

Néhány klasszikus kódolási módszer bemutatása:
www.ftech.net/~monark/crypto/crypt/crypt.htm
Az Enigmáról:
www.attlabs.att.co.uk/andyc/enigma/about_enigma.html
www.cs.miami.edu/~harald/enigma/enigma.html
Az RSA eljárás matematikai hátteréről:
dslab.csie.ncu.edu.tw/~lucas/rsamath.HTM
Windows 2000 High Encryption Pack:
www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp
Internet Explorer High Encryption Pack:
www.microsoft.com/windows/ie/download/128bit
A böngésző titkosító képességének ellenőrzése:
www.fortify.net/sslcheck.html
A Windows 2000 kriptográfiai szolgáltatásai:
msdn.microsoft.com/isapi/msdnlib.idc?theURL=/library/psdk/crypto/cryptovrvw_8395.htm
Biztonsági technológiák a Windows 2000-ben
www.microsoft.com/windows2000/library/technologies/security/default.asp

Hitelesség 2000 után Smart Card alkalmazásával

Keleti Arthur
akeleti@icon.hu

A titkosítást és hitelesítést megvalósító rendszerekben az egyik leggyakoribb gond a kulcsszavak biztonságos tárolása. A Windows 2000 javított biztonsági szolgáltatásai és a Smart Cardok beépített támogatása kiváló megoldási lehetőséget kínál.

A felhasználók hitelességét bizonyítani tudó eljárások iránt az utóbbi évtized során egyre komolyabb kereslet támadt.

A szoftvergyártók gyorsan reagáltak az érdeklődésre, a piac ma egy sor nyilvános kulcsú titkosítást alkalmazó informatikai biztonsági szoftverrel dicsekedhet, melyek között vannak ígéretes és kevésbé ígéretes, ingyenes és súlyos dollárezrekbe kerülő termékek is.

A növekvő informatikai bűnözés hatására az informatikai biztonság, és annak operációs rendszerekbe integrált alkalmazási lehetőségei egyre inkább a figyelem középpontjába kerülnek. Úgy tűnik, az új évezred első éveiben az operációs rendszerek fejlesztése során az erős felhasználó-hitelesítés iránti jogos igény kulcsszerepet kap.

A 2000 első negyedévében útjára bocsátott Windows 2000 informatikai biztonsági megoldásai is az erős hitelesítést és az adatok titkosítását állítják középpontba.

E megoldások valós lehetőséget nyújtanak arra, hogy a felhasználók a hagyományos, jelszavas azonosításnál jóval szigorúbb biztonsági ellenőrzés mellett használhassák a rendszer erőforrásait (lásd még a *A Windows 2000 biztonsági szolgáltatásai* című cikkünket).

A Windows 2000 informatikai biztonsági megoldásait (eltérően az NT 4-től) gondosan a már létező azonosítási szabványokra és protokollokra építették. Az új rendszerben az NTLM (Windows NT Lan Manager) helyett az Internet-szabványos (RFC 1510) Kerberos 5.0 az alapértelmezett azonosítási protokoll. A protokoll 5.0-s verzióját 1993-ban fejlesztették ki, és azóta is elterjedten használják más operációs rendszerekben (pl.: Sun Solaris). Ennek eredményeképpen az azonosítási rendszer nagyon megbízhatóvá és – az informatikai biztonság szűkre szabott keretein belül – rugalmassá vált. A korábbi módszerrel szemben az új megoldás a kapcsolat mindkét résztvevőjét képes egymás számára erős hitelesítéssel azonosítani, és mindemellett a hálózati kapcsolatok kiépítésének folyamata is felgyorsult.

A Kerberos protokoll neve a görög mitológiából származik. Hitvilágukban Kerberos, a háromfejű kutya őrizte az alvilág kapuját. Nevéhez méltón a protokoll a kliens és a szerver (a kutya két feje) között harmadik fejként közvetít. Ez a harmadik, köztes résztvevő a KDC (Key Distribution Center – kulcselosztó központ), melyben mind a szerver, mind pedig a kliens megbízik, és elfogadja ítéletét a másik hitelességére vonatkozóan.

A KDC szervizként fut egy különálló biztonságos szerveren. Feladata, hogy nyilvántartsa az összes azonosításra szoruló és elérhető hálózati résztvevőt (legyen az felhasználó, szerver vagy bármilyen szolgáltatás), és közöttük közvetítsen.

Amikor például valamelyik kliens az egyik szerverhez szeretne kapcsolódni, felveszi a kapcsolatot a KDC-vel, amely mindkettejük számára kiad egy-egy titkosító kulcsot (session key) és azonosító tantuszt (ticket), amelyet a két résztvevő az egymás közötti kapcsolatfelvételhez használ.

Ezen kívül a KDC tárolja a (szimmetrikus titkosításon alapuló) hitelesítés mindegyik résztvevőjének (felhasználó, szerver, szolgáltatás stb.) titkos jelszavát (ennek eredetije a kulcs tulajdonosánál – a hitelesítés egyik résztvevőjénél – van). Ez a kulcs (long-term key) az azonosítás korai szakaszában a KDC és az azonosításban résztvevő másik fél közötti titkosított kommunikációra szolgál.

Kerberosos és smart cardos bejelentkezés a Windows 2000-ben

A Windows 2000-ben a Kerberos protokoll felel a felhasználók azonosításáért is. Ez a gyakorlatban azt jelenti, hogy a felhasználók hitelesítése a KDC és a felhasználók közötti párbeszéden keresztül történik. Az ilyen párbeszédekben a KDC meggyőződik arról, hogy a felhasználó birtokolja-e a belépéshez szükséges kulcsot (long-term key).

A kulcs a felhasználó által megadott jelszóból képződik és ezt a KDC összehasonlítja a saját listájával (ugyanis a felhasználó jelszavának létrehozásakor a KDC is kap egy másolatot róla). Ha a kulcsok egyeznek, a KDC engedélyezi a felhasználó hozzáférését.

A jelszó megadásával létrehozott kulcs valójában annak a szimmetrikus titkosítási eljárásnak a része, amely a KDC és a felhasználó közötti adatváltást rejti el az avatatlan szemek elől (amit a KDC a felhasználónak szán, azt a felhasználó kulcsával kódolja).

A Windows 2000-ben alkalmazott Kerberos protokoll azonban lehetőséget teremt arra is, hogy az alacsonyabb informatikai biztonságot nyújtó szimmetrikus titkosítás helyett aszimmetrikus titkosítást használjunk a felhasználók azonosítása során. Ezt a Kerberos public key infrastructure-ön keresztül valósítja meg. Ebben az esetben adott felhasználó azonosításához a KDC kizárólag a felhasználó kulcspárjának nyilvános darabját használja fel, míg a felhasználó a kulcspár titkos darabjával dolgozik.

A rendszer része még a CA (Certificate Authority – tanúsítvány-hitelesítő) is, ez a kulcspár tulajdonosának (felhasználójának) adatait és jogait rendeli össze magával kulcspárral.

A kulcspár publikus darabja, valamint a tulajdonos adatai és jogai együtt alkotják a certificate-et, amelyet a CA aláírásával hitelesít. A CA tartja nyilván az érvényüket vesztett és visszavont tanúsítványokat is.

A Windows 2000 azt is támogatja, hogy a Kerberos 5.0 nyilvános kulcsú kiterjesztését alkalmazva a felhasználók titkos kulcsát intelligens chipkártyán tároljuk.

A chipkártyaolvasón keresztül csatlakoztatott Smart Cardot az operációs rendszer képes magától lekezelni.

Az Icon Hydra nevű Smart Card csomag is erre a rendszerbe integrált funkcióra épül. *(A mitológiai Kerberosnak volt néhány testvére, Hydra is közéjük tartozott. Elszánt, erős sárkány-kígyónak tartották, akinek egyes elbeszélések szerint kilenc feje volt.)*

A csomagban található chipkártya olyan kriptokártya, amely a Kerberos-azonosításhoz szükséges felhasználói titkos kulcsot az azonosítás során a kártya memóriájából bocsátja rendelkezésre. A chipkártya intelligenciájának köszönhetően a titkos kulccsal kapcsolatos műveletekhez a kulcsnak nem kell elhagynia a kártyát, az operációs rendszer közvetlenül azt utasítja az azonosításhoz szükséges kriptográfiai műveletek végrehajtására. Mivel mind publikus, mind titkos kulcsunk a kártyán tárolódik, az azonosítási folyamat megkezdésekor a Windows 2000-nek is a kártyához kell fordulnia. Ehhez természetesen a felhasználónak meg kell adnia a – jelszóhoz hasonló – PIN-kódját. Ez védi ugyanis a felhasználó kriptokártyáját az illetéktelen használattól.

A helyes PIN-kód megadása után a Windows 2000 a kriptokártyához fordul, lekéri a felhasználó nyilvános kulcsát (ez X.509-es formátumú tanúsítvány), és ezzel titkosítja a felhasználónak szánt üzeneteit. Ebben az esetben tehát a felhasználót a nyilvános kulcsú rendszerben a titkos kulcsa egyértelműen hitelesíti.

A Smart Card hatalmas előnye, hogy semmiképp sem szerezheti meg más a kártyában rejtőző titkos kódot, ugyanis az sosem hagyja el a kártyát. Azaz megszemélyesítés csak a kártya ellopásával lehetséges, ez azonban közvetlen fizikai kontaktust igényel, és feltűnő, nem úgy, mint az Internet távoli szegletéből végzett elektronikus betörés. Ráadásul nem elég ellopni a kártyát, a PIN-kódot is ismerni kell az illegális használathoz!

Szabvány	Miről szól?	Miért fontos?
X.509 version 3	Certificate-ek (tanúsítványok) formátuma és tartalma	Segítségével a felhasználó személye és a számára elkészített kulcspár rendelhető össze. Általános szabványt határoz meg a különböző gyártók alkalmazásai között folyó tanúsítvány cserékre és hitelesítésekre
CRL version 2	A bevont certificate-ek (tanúsítványok) listájának (revocation list) formátuma és tartalma	Ennek segítségével a tanúsítványellenőrzési folyamatokat végző alkalmazások (vagy maga az operációs rendszer) ellenőrizhetik a tanúsítványok érvényességét
PKCS family	A nyilvános kulcs cseréjének és terjesztésének formátuma és módja	Egymástól független, különböző gyártók e szabvány segítségével szabályozott módón mozgathatják a nyilvános kulcsot, alkalmazásaik „összedolgozhatnak"
SSL version 3	Titkosított és hitelesített internetes kommunikáció	Az SSL-t internetes/intranetes környezetben használják kliens és szerver hitelesítésre, illetve a köztük zajló kommunikáció titkosítására
IPSec	Az Internet Protocol (IP) beépített, csomagszintű titkosítást használó továbbfejlesztése	Az IPSec segítségével transzparensen és automatikusan titkosíthatjuk a hálózati adatforgalmat
PKINIT	Nyilvános kulcsok használatát írja le hálózati bejelentkezésekhez a Kerberos hitelesítési protokoll segítségével	A Kerberos azonosítja a felhasználókat a hálózaton, a PKINIT lehetővé teszi, hogy a Kerberos Smart Cardokon elhelyezett tanúsítványokat használjon erre a célra
PC/SC	Szabvány Smart Cardok és számítógépek összekapcsolásához	A Windows 2000 operációs rendszer szinten nyújt támogatást a Smart Cardoknak

Néhány Windows 2000 által támogatott PKI szabvány

„Kulcskovácsolás“

Az Icon Hydra által használt chipkártyán a kriptográfiai műveletekért felelős egyedi chip látja el a titkosítási és kulcskészítési feladatokat. A Windows 2000 a chip funkcióit használja arra is, hogy a chipkártya felhasználója számára elkészítse a nyilvános kulcsú műveletekhez szükséges kulcspárt (RSA módszer szerint).

A kulcskészítés során a kulcspár titkos darabja a chipkártyán „születik“, és soha sem hagyja el azt. Ezáltal sem a kulcsot elkészítő, sem a kulcs tulajdonosa nem ismeri a kulcs pontos tartalmát, mégis tudja használni.

A kártyán kívül még a tanúsítványok kiadásáért felelő CA (Certificate Authority – tanúsítvány-hitelesítő – lásd még *Biztonságos honlap Certicate Serverrel* című cikkünket) szerverer a kulcskészítési folyamat résztvevője.

A kártya által generált kulcspár nyilvános darabjához a hitelesítő az X.509 szabványnak megfelelően a felhasználó személyével és jogosultságaival kapcsolatos információkat fűzi hozzá, valamint nyilvántartja a kiadott, illetve visszavont tanúsítványokat.

A Smart Card egyéb felhasználási területei a Windows 2000-ben

Miután titkos kulcsunk a kriptokátyán már megfelelően védett környezetben várja, hogy felhasználjuk, elgondolkodhatunk azon is, hogy a nyilvános kulcsú titkosítást milyen egyéb feladatokra tudjuk „befogni“. Az operációs rendszer nemcsak az azonosításhoz képes használni a kártyát, hanem bármilyen alkalmazás számára is elérhetővé teszi szolgáltatásait. Íme néhány példa a lehetséges felhasználások közül:

Biztonságos e-mail

A Windows 2000-ben az elektronikus levelezés biztonságossá tételére az RSA ajánlására épülő S/MIME 2-t, illetve ennek továbbfejlesztését, az Internet Engineering Task Force (IETF) S/MIME 3 eljárását alkalmazzák. Ennek segítségével a levelek tartalma is titkosítható (data encryption) és a küldő személye is ellenőrizhető (digital signature).

Az Icon Hydra intelligens kriptokártyája biztosan őrzi titkos kulcsunkat

• **Digitális aláírás (Digital Signature)**

A kriptokártyán található titkos kulccsal olyan aláírást tudunk készíteni leveleinkre, amely teljesen egyedi és csak ránk jellemző. Az ilyen digitális aláírás nemcsak a felhasználó hitelességét, hanem az aláírt dokumentum érintetlenségét is bizonyítja, tehát a címzett biztos lehet benne, hogy a feladó az, akinek mondja magát, és amit írt, változtatás nélkül jutott el hozzá. A digitális aláírás felhasználható a vállalati elektronikus levelezés hitelességének igazolására. Amennyiben (pl.: valamely szervezeti intranetes környezetben) kötelező minden elektronikus levélre digitális aláírást elhelyezni, az elektronikus levelezés egyértelműen hivatalossá tehető.

• **Adattitkosítás (Data Encryption)**

A címzett nyilvános kulcsát felhasználva olyan levél írható, amelyet csak és kizárólag a címzett tud majd elolvasni a csak és kizárólag a kriptokártyán tárolt titkos kulcsa segítségével. Ilyen adattitkosítási megoldás alkalmazásával a vállalati levelezés, illetve az érzékeny adatok cseréjének informatikai biztonsági szintje nagyságrendekkel emelhető.

Ezek a funkciók az S/MIME-ot alkalmazó levelező rendszerekben, például az Outlook levelezőkliens használatával érhetők el.

Webbiztonság (Web Security)

A nyilvános kulcsú titkosítás és a Smart Cardok használata a webes információk (és azok hordozóinak) hitelesítésében is jelentős szerepet játszhat.

A Windows 2000 alapvető webbiztonsági megoldásként SSL-t (Secure Socket Layer), valamint TLS-t (Transport Layer Security – az IETF ajánlása) használ. Ezek a protokollok gyakran kapcsolódnak az ismert webtartalom-hordozó protokoll, a HTTP nevéhez is (HTTPS – Secure HTTP). Felhasználásukkal a következő funkciókat érhetjük el:

- Szerverazonosítás – a kliensek ellenőrizhetik annak a szervernek a hitelességét, ahonnan az adatokat kapják.
- Kliensazonosítás – a szerverek ellenőrizhetik azon kliensek hitelességét, amelyek tőlük adatokat töltenek le.
- Titkosítás – a szerverek és kliensek közti adatforgalom titkosítható.

Ahhoz, hogy minden funkciót teljes mértékben ki tudjunk használni, mind a felhasználónak (kliensnek), mind pedig a szervernek rendelkeznie kell érvényes kulcspárral, illetve megbízható (CA által kiállított) tanúsítványokkal. Egymás tanúsítványainak cseréjével a kommunikációban résztvevő felek meg tudják állapítani egymásról, hogy hitelesek-e. A felhasználó saját hitelességét a szerver felé a kriptokártyáján tárolt titkos kulcs használatával tudja igazolni.

A hitelesség elfogadását követően a felhasználó és a szerver újabb kulcs használatában állapodhatnak meg, azután ezzel titkosíthatják a kettejük közötti adatforgalmat.

File-rendszer titkosítása (EFS – Encrypting File System)

A Windows 2000 EFS támogatja a file-ok valósidejű titkosítását és dekódolását a Windows NT-ből már jól ismert NTFS file-rendszerben. Megfelelő EFS tanúsítványok birtokában (ezt a CA szerver állítja elő) a felhasználók képesek adatállományaikat titkosítani, illetve azokat igény szerint dekódolni.

Az adatállomány titkosítása során az EFS új (véletlenszerű) titkos kulcsot állít elő, amellyel az állományt kódolja. Ezt a kulcsot a felhasználó nyilvános kulcsával titkosítva tárolja, így lehetővé teszi, hogy csak a titkosítást kérő személy férhessen az állományhoz, és csakis abban az esetben, ha titkos kulcsával dekódolni tudja az EFS által számára elkészített és titkosított kulcsot. Az állományok visszaállításáért felelős személyek megfelelően szabályozott módon szintén kaphatnak egy-egy – természetesen saját nyilvános kulcsaikkal titkosított – másolatot az EFS által előállított kulcsból.

Az Icon Hydra műszaki adatai

Icon Hydra Smart Card

- ISO 7816 szabványra épül
- RSA 512, 768 vagy 1024 kulcskészítés a kártyán
- DES 56 és 112 bit kulcskészítés a kártyán
- SHA-1 hash támogatás
- MD5 hash támogatás
- DES és Triple DES MAC támogatás (56, 112 bit kulcshosszúságig)
- DES és Triple DES MAC Chain Block Chiper (56, 112 bit kulcshosszúságig)
- Titkosított kulcs feltöltés (DES és RSA)
- EMV kompatibilis
- PC/SC-vel integrálható
- PKCS#11-gyel integrálható
- Felhasználható memória: 7900 byte
- Kommunikációs sebesség 9 600 bit/s-tól 153 000 bit/s-ig

Icon Hydra Smart Card olvasó

- Fogyasztás ISO 7816 és EMV szabvány szerint (5V, 100mA)
- 9 tűs RS232 soros port csatlakozás (az áramot a billentyűzetről veszi)
- PC/SC kompatibilis
- EMV kompatibilis
- Chipkártya és olvasó rövidzárlat-védelem
- Kommunikációs sebesség 9 600 bit/s-tól 153 000 bit/s-ig

Biztonságos távoli elérés (Secure RAS – Remote Access)

A megfelelő kulcsok alkalmazásával a Dial-up (betárcsázásra épülő) kapcsolatok is erős hitelesítéshez köthetők. Ez a gyakorlatban azt jelenti, hogy adott távoli elérés kiépítése során (pl.: tárcsázás otthonról a vállalati intranetbe) a hagyományos felhasználó név és jelszó helyett a kriptokártya segítségével tudunk belépni. Ezt a megoldást alkalmazva a belső hálózat biztonsága nagymértékben javítható, ha távoli eléréssel csatlakozó munkatársakat vagy külső partnereket engedünk be.

Biztonságos virtuális magánhálózat (Secure VPN – Virtual Private Network)

Virtuális magánhálózat kiépítésével két vagy több szervezeti hálózat biztonságos alacsonyabb biztonsági szintet nyújtó közegen (pl.: nyilvános hálózat – Internet) keresztüli összekapcsolása valósítható meg. Erős hitelesítés a magánhálózat kapcsolatainak felépítéséhez és fenntartásához szintén használható. Ebben az esetben a VPN felépülésének feltétele a hagyományos jelszóalapú azonosítás helyett a kriptokártya felel kilétünk bizonyításáért. A virtuális magánhálózatban elengedhetetlen az adatok megfelelően nagy biztonsági fokú titkosítása.

Összegzés

Az operációs rendszerekben, az azokon futó alkalmazásokban megfelelően használt nyilvános kulcsú titkosításra épülő megoldások talán képesek lesznek eloszlatni a hitelességgel kapcsolatos kételyeinket.

Valószínű, hogy a már sikeresen alkalmazott, és a rendszerek között nagy fokú kompatibilitást megteremtő szabványok használata nagyban elősegítheti az adat- és hitelességvédelem fejlődését.

Ez olyan folyamat, amelyben meg kell szoknunk, hogy személyazonosságunkat mindenhol és mindenkivel szemben igazolnunk kell, hogy adatainkat vagy leveleinket rendszeresen titkosítjuk, s mindehhez apró, műanyaglapocskákat használunk mind a bankautomatánál, mind a számítógépünk előtt.

Hogy ez kényelmetlen? Talán, egyelőre... De várható, hogy a jelen és a közeljövő operációs rendszerei egyre kimagaslóbb támogatással sietnek majd segítségünkre e téren is. A Windows 2000 e fejlődés fontos lépcsője lehet.

Mutatók

www.microsoft.com/windows2000/library/technologies/security/default.asp
www.isi.edu/gost/publications/kerberos-neuman-tso.html
www.contrib.andrew.cmu.edu/~shadow/kerberos.html
www.ietf.org/rfc.html

Lépcsőzetes frissítés a Windows 2000 rendszerre

Az egyéni igények és lehetőségek függvényében a Windows 2000-et többféle lépcsőzetes módszerrel is be lehet vezetni.

Nem szükséges azon nyomban az összes kiszolgálót lecserélni, és bevezetni az Active Directoryt. Megtehetjük, hogy csak a klienseket frissítjük Windows 2000 Professionalre, vagy kibővítjük szerverparkunkat néhány új Windows 2000-es géppel. Érdemes megfontolni, hogy cégünknek pontosan melyik új szolgáltatásra van szüksége, és ez alapján célszerű eldönteni, hogy melyik gépeket érdemes fejleszteni.

Ha a felhasználóink igénylik a Windows 2000 újdonságait, érdemes először a kliensgépeken frissíteni. Ezután – megtartva az NT 4 domain rendszerét – nekiláthatunk a kiszolgálók frissítésének, annak rendje és módja szerint az alkalmazás-, a file- és a nyomtatószerverekkel az élen. Ha már minden feltétel adott, érdemes az NT-tartományokat az új Windows 2000 tartományi architektúrára frissíteni, hogy a legizgalmasabb új szolgáltatások, például az Active Directory előnyeit is élvezhessük.

Amellett, hogy közvetlen előnyöket is nyújt, az Active Directory a Windows 2000 számos új szolgáltatásának igénybevételéhez is szükséges. Ha jelenlegi rendszerünk egyszerű – például egyetlen NT 4 tartományból áll –, a Windows 2000 varázslói segítségével könnyen és gyorsan átállhatunk az Active Directoryra. Ha a környezet összetettebb, több tervezésre lesz szükség, de néhány jól használható eszköz ebben is a segítségünkre siet.

Windows 2000 Professional

A Windows 2000 Professional jól beilleszkedik a már meglevő rendszerkörnyezetbe, és egyszerűen telepíthető a legtöbb korábbi Windowsra. Figyelembe véve a felhasználók igényeit és az elérhető hardverkonfigurációkat akár egyenként is frissíthetjük a kliensgépeket.

Windows 2000 Server

Az Active Directory a Windows 2000 szerververzióinak egyik leghasznosabb újítása, de akkor is érdemes upgrade-elni kiszolgálóinkat, ha nem akarjuk, vagy nem tudjuk véghezvinni a bevezetéséhez szükséges teljes átalakítást. Érdemes lehet akár egy-egy NT 4 alatt futó tagkiszolgálót is frissíteni, ugyanis jelentős javulást tapasztalhatunk a megbízhatóság és kezelhetőség terén, ezen kívül jó néhány új szolgáltatásra is szert tehetünk.

A tagkiszolgálók (member server) azok a számítógépek, amelyek a file-, nyomtató-, web- és alkalmazás-kiszolgáló feladatokért felelősek. Valójában a tartományvezérlők kivételével a hálózat minden szervere tagkiszolgáló. Az alábbi táblázat a Windows 2000 azon legfontosabb szolgáltatásait tartalmazza, amelyek az Active Directory telepítése nélkül is elérhetők.

Az NT 4-es szerverek egyszerűen frissíthetők Windows 2000-re. Azért is jó ötlet néhány szervert frissíteni, mert így megismerkedhetünk a Windows 2000 rendszerrel, és az Active

A szerver típusa	A Windows 2000 új szolgáltatásai
File- vagy nyomtatószerver	Lemezkvóták; dinamikus kötetkezelés; hierarchikus tárkezelés; internetes nyomtatás
Web- vagy alkalmazásszerver	IIS 5.0, XML, COM+ és terminál-szerviz; nagy üzembiztonságot lehetővé tevő szolgáltatások
Kommunikációs szerver	Virtuális magánhálózat (VPN); távelérési (RAS) szolgáltatások; IP-telefon; RADIUS hitelesítés és fiókkezelés
Infrastrukturális szerver	Távmenedzsment; nyilvános kulcs infrastruktúra (Public Key Infrastructure); rendszerbeállító eszköz (System Preparation Tool)

Directory telepítésének megtervezéséhez már tapasztaltan foghatunk hozzá.

Windows 2000 Active Directory

Az Active Directory segítségével az alkalmazások, a felhasználók, az adatok és más erőforrások egységes környezetbe illeszthetők.

Az – egyre nagyobb számban elérhető – Active Directoryt támogató alkalmazásokat egyszerűbb telepíteni és karbantartani, ugyanis nem kell egyenként vesződni az alkalmazások saját címtárszolgáltatásával. A karbantartás egyszerűsödése mellett a rendszer biztonsága és az alkalmazások együttműködése is javul az Active Directory jóvoltából.

Az Active Directory hatékony bevezetéséhez az alapos, előzetes tervezés nélkülözhetetlen. Erre a szakaszra érdemes hosszabb időt szánni, mert így elkerülhető, hogy a későbbiek során a már kész struktúrák újraépítésére kelljen felesleges időt és pénzt áldozni (lásd még az *Áttérés* című cikket).

Ha – a rendelkezésre álló varázsló segítségével – upgradeeljük NT 4-es rendszerünk elsődleges tartományvezérlőjét (PDC, Primary Domain Controller), máris kihasználhatunk olyan Active Directory szolgáltatásokat, mint például a kliensgépek adminisztrációját elősegítő IntelliMirror technológia.

Az Active Directory messzemenőkig kompatibilis a már meglévő NT-alapú környezettel. A migráció idejére a tartalék tartományvezérlőkön (BDC, Backup Domain Controller) például meghagyhatjuk az NT-t, a frissített tartományvezérlők pedig továbbra is támogatják a Windows 9x/NT-s klienseket.

Idővel, ahogy a terveink és a szerverek bővítése engedi, érdemes a BDC-ket Active Directory tartományvezérlőkké előléptetni. Az elérhető technikai útmutatók és eszközök segítségével a teljes átállás aránylag kockázatmentesen elvégezhető, és ha szükséges, a frissítés bármelyik pontján vissza lehet állítani a rendszert az NT-tartományok használatára.

Az Active Directory egyedi telepítése

A Windows 2000 Server és az Active Directory szolgáltatásainak teljes skálája csak akkor érhető el, ha már a tartomány valamennyi tartományvezérlőjét frissítettük. Ekkor a – például az NT 4-es tartományvezérlőkkel való – visszamenőleges kompatibilitás megteremtése céljából betartott korlátozások megszűnnek. Az új rendszer néhány tulajdonsága olyan vonzó, hogy érdemes megfontolni az egyszerű frissítés helyett a bonyolultabb tartomány-újraépítés végrehajtását.

A tartományfrissítés során az a cél, hogy a pillanatnyi környezeten a lehető legkevesebb változtatást kelljen végrehajtani, beleértve az adott tartomány szerkezetét is. A tartomány-újraépítés ezzel szemben arra irányul, hogy a szerkezet átalakításával a tartomány felépítését minél inkább a cég igényeihez igazítsuk.

A tartomány újraépítése többféleképpen is elvégezhető, de a végeredmény általában a kiinduló állapotnál áttekinthetőbb, hiszen kisebb számú, viszont nagyobb méretű tartománnyal rendelkező struktúrát kapunk.

Az újraépítésre háromféle helyzetben kerülhet sor.

- **Frissítés után**: – általában a Windows 2000-re történő átállás második lépéseként célszerű elvégezni a tartomány-újraépítést. Ha a frissítés során az egyszerűen átalakítható részekkel már megbirkóztunk, ebben a lépésben a cél egyrészt a hálózati infrastruktúráért felelős tartományrészek leegyszerűsítése, másrészt az NT domainek beágyazása az Active Directory szerkezetébe.
- **Frissítés helyett**: – egyes cégek nem engedhetik meg maguknak, hogy fokozatos átállással veszélyeztessék meglévő üzemi környezetük stabilitását. Ebben az esetben érdemes lehet a jelenlegi rendszertől függetlenül kialakítani egy ideális Windows 2000 Active Directory-alapú környezetet.
- **Átállás után**: – előfordulhat, hogy már a véglegesen Windows 2000-re átállított hálózatban kell átalakítani a tartományokat. Erre akkor kerülhet sor, ha valamilyen okból – például változás a cég felépítésében: egyesítés vagy felvásárlás – az adott szerkezet már nem megfelelő.

Újraépítést leginkább azért érdemes végrehajtani, hogy kihasználhassuk a Windows 2000 azon szolgáltatásait, amelyek segítségével jobban a cég igényeihez illeszthetjük rendszerünket. Ilyen igények a következők lehetnek:

- **Jobb méretezhetőség**: mivel az Active Directory a szó szoros értelmében több millió felhasználói fiók kezelésére képes, az NT-tartományok helyett kevesebb, de nagyobb tartományt alakíthatunk ki.
- **Pontosabban meghatározható felügyeleti jogok**: sok esetben megkönnyíti a felügyeleti jogok kiosztását, ha az NT erőforrás-tartományokat Active Directory szervezeti egységekké (OU) alakítjuk át.
- **Egyszerűbb rendszerfelügyelet**: azért, hogy a felügyeleti jogok átruházhatók legyenek, vagy mert korábban cégünk szervezete jelentős változáson (például felvásárlás) ment át, elképzelhető, hogy jelenlegi tartományszerkezetünk bonyolultan egymásba fonódó meghatalmazási kapcsolatokból áll. Az újratervezéssel elérhetjük, hogy kevesebb legyen a kétirányú tranzitív meghatalmazási kapcsolat.

Az ADMT (Active Directory Migration Tool) leegyszerűsíti az újraépítés végrehajtását, akármelyiket is választjuk a fenti lehetőségek közül. Emellett lehetővé teszi, hogy fenntartsuk a már meglévő tartományszerkezetet az újraépített környezettel párhuzamosan. Így ha az újraépítés bármely szakasza esetleg nem a kívánt eredményt hozza, az eredeti konfiguráció gyorsan visszaállítható.

Mutató

Windows 2000 Server Deployment and Planning Guide
www.microsoft.com/technet/win2000/dguide/home.asp

Áttérés

Kozári Ákos
akosk@microsoft.com

Áttérés. A döntés meghozatalát követően ez a szó, illetve a mögötte megjelenő stratégiai kérdések, tervezési, előkészítési és végrehajtási tevékenységek az elkövetkező időszakban igen fontos kérdéskört fognak jelenteni a cégek, vállalatok, illetve azon belül az informatikai szervezetek számára.

Figyelembe véve a Windows 2000 operációs rendszer architektúrájában történt változásokat, a funkcionalitás nagyarányú kiterjedését, a kérdéskört más kontextusban kell kezelnünk.

Az áttérés részben szakmai informatikai feladat, ahol a jelenleg alkalmazott Windows NT 4.0 alapú hálózati infrastruktúra migrációjáról beszélhetünk.

Másrészről azonban az új operációs rendszer funkcionális lehetőségei, illetve az arra támaszkodó, továbbiakban kibocsátásra kerülő alkalmazások kapcsán a vállalatok, cégek számára új informatikai támogatási, megoldási lehetőségek jelennek meg.

Az új lehetőségek figyelembe vétele, kihasználása stratégiai kérdés. A stratégiai tervezési, valamint migrációs feladatokat az áttérés kapcsán szoros összefüggésben kell vizsgálnunk. Ezek figyelembe vétele a sikeres, előre mutató áttérés kulcsa.

A stratégiai tervezés elvégzését követően a Windows 2000 alapú informatikai architektúrára történő áttérés első gyakorlati lépése a vállalatok jelenlegi informatikai infrastruktúrájának migrációja. Ez a kiépített informatikai infrastruktúrától függően igen összetett feladathalmazt is jelenthet, amely gondos tervezést, előkészítést igényel. Az alábbiakban ennek a feladatkörnek az áttekintésével foglalkozunk, amelyet egy általános Windows 2000 infrastruktúra kialakítási procedúrával párhuzamosan vizsgálunk.

Mire legyünk figyelemmel?

A bevezetésben már kiemeltük a vállalat üzleti tevékenységének támogatásával kapcsolatos tervezési feladatokat.

Az áttéréssel kapcsolatban ezen túl a következők megtervezésére, kidolgozására van szükség:

- Active Directory névstratégia kialakítása.
- A tartományok topológiájának kialakítása, tartomány-frissítési, tartomány átszervezési koncepció kidolgozása, tervezése.
- A jelenlegi névfeloldási (DNS) szolgáltatás és topológia alkalmazhatóságának vizsgálata, szükség esetén átalakítása.
- A Windows 2000 telephelyek (site-ok) közötti kommunikáció tervezése.
- Szoftver- és hardver-kompatibilitási kérdések vizsgálata.
- A frissített rendszerre vonatkozó üzemeltetési eljárás, illetve katasztrófa elhárítási forgatókönyv kidolgozása.

Active Directory névstratégia kialakítása

Az Active Directory szolgáltatás névterületéhez (namespace) tartozó tartományok DNS névkezelési alapokra támaszkodnak. Emiatt a Windows 2000 tartományok nevei egyben DNS tartományok nevei is. Minden Windows 2000 tartomány számára szükséges tehát, hogy rendelkezésre álljon egy megfelelő DNS tartomány.

Abban az esetben, ha még nem áll rendelkezésre megfelelő DNS tartományi struktúra, annak létrehozásával kapcsolatban a következő szabályok, ajánlások figyelembevétele szükséges:

- A tartományok nevei nem lehetnek 63 karakternél hosszabbak. Az FQDN teljes hossza maximálisan 255 karakter.
- Egyedi tartományneveket alkalmazzunk. Minden altartomány nevének egyedinek kell lennie a vonatkozó tartományban.
- Limitáljuk a tartományi hierarchia mélységét. (Ne hozzunk létre 5 szintnél mélyebb tartományi hierarchiát!)

- Egyszerű tartományneveket válasszunk.
- Szabványos DNS (a-z, A-Z, 0-9, -) (lásd RFC 1123, RFC 952), illetve UNICODE (lásd RFC 2044) karaktereket alkalmazzunk! (A Windows 2000 nem különbözteti meg a kis- és nagybetűket.)

Az Active Directory tartományi struktúra kialakításával kapcsolatban lehetőség van már létező, a vállalat számára korábban már kialakított DNS tartományi struktúra implementálására is.

Az Active Directory szolgáltatások támogatásához a DNS kiszolgálónak az alábbi jellemzőkkel kell rendelkeznie:

- Service location resource record támogatás (RFC 2052 alapján);
- Dynamic update protocol for DNS támogatás (RFC 2136).

A Windows 2000 operációs rendszerben található DNS szolgáltatás optimálisan kielégíti ezeket a feltételeket (Ezen túl a titkosított, inkrementális zónatranszfer szolgáltatás szintén rendelkezésre áll.).

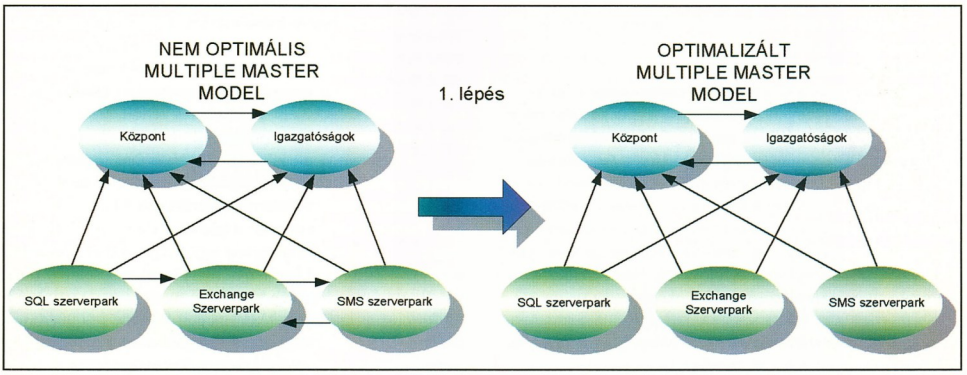
Tartományok topológiájának kialakítása, frissítési lehetőségei

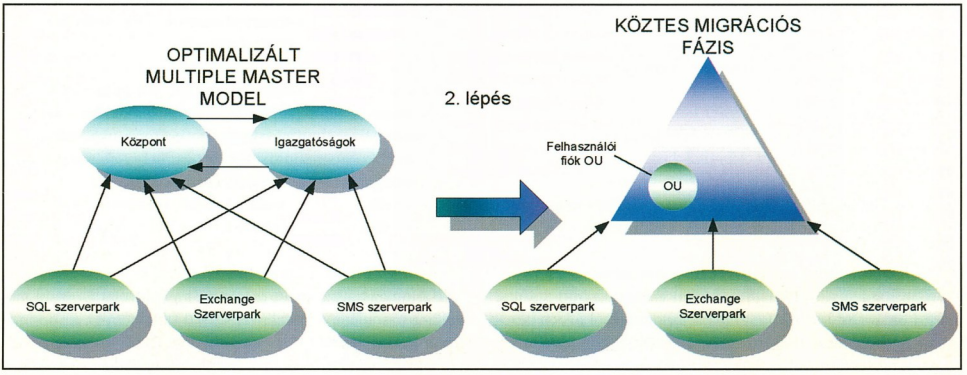
A Windows 2000 operációs rendszer-alapú infrastruktúrára történő áttérést két fő koncepció alapján – tartományfrissítéssel (helyben végzett frissítés), vagy tartományátszervezéssel (tartományok egyesítése, tartományok összevonása) – végezhetjük el.

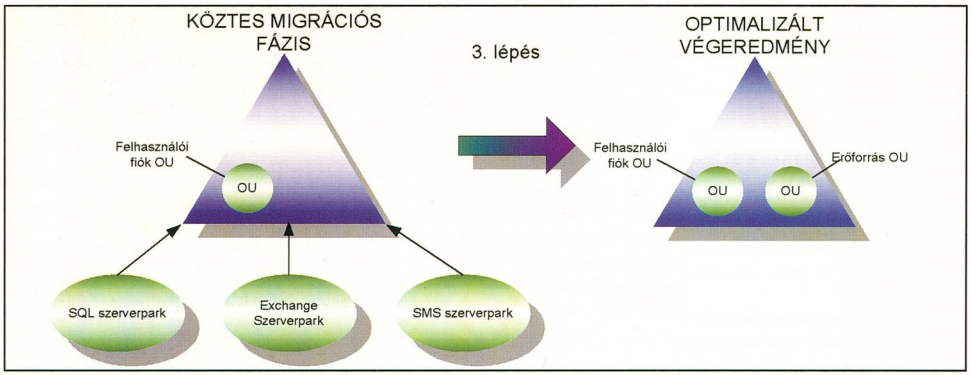
A választandó koncepció a jelenleg alkalmazott tartományi modelltől, valamint a kívánt, optimalizálandó informatikai infrastruktúra jellegétől függően változhat. Bár a tartományfrissítési koncepció egyszerűbb folyamat, az esetek többségében a tartományátszervezési koncepció az ideális választás.

Az alábbi ábrákon egy lehetséges átszervezési megoldást mutatunk be egy nem megfelelően kialakított Windows NT 4.0 alapú tartományi topológiára vonatkozóan:

Az 1. lépésben a Windows NT 4.0 alapú tartományi topológia optimalizálására kerül sor. A folyamat végeredményeként







egy megfelelően paraméterezett Multiple Master tartományi modell jelenik meg.

A 2. lépésben a már optimalizált Windows NT 4.0 tartományi topológiából a felhasználói fiókokat tartalmazó tartományok migrációjára kerül sor.

A felhasználói fiókok a Windows 2000 tartomány szervezeti egység tárolóba (Organization Unit) kerülnek át. Az erőforrás-tartományokban található számítógépek (például alkalmazás-kiszolgálók) egyirányú megbízotti kapcsolattal csatlakoznak a Windows 2000 tartományhoz.

A 3. lépésben kerül sor a fennmaradó Windows NT 4.0 tartományok migrációjára. Ebben az esetben az erőforrás tartományok egy szervezeti egység tárolóba (OU) kerülnek át. Optimalizált végeredményként egy egyszerű, jól adminisztrálható tartományi topológia áll rendelkezésünkre.

A tartományok átszervezése esetén célszerű a minél egyszerűbb tartományi topológia megvalósítása.

A tartományi topológia összetettebb (több tartományt tartalmazó) kialakítását az alábbi szempontok indokolhatják:

- Adminisztratív szempontok (kizárólagos adminisztrációs igények egy adott szervezeti egységre, vagy tartományra vonatkozóan).
- Eltérő security policy.
- Replikációs határok figyelembe vétele lassú vonali kapcsolatok esetén.

A vállalat jelenlegi Windows NT tartományi modelljétől függően különböző frissítési modellek alkalmazhatók:

1. Single Domain modell

Kialakítását és a migrációs feladatokat tekintve a legegyszerűbb modell. E tartományi modell esetén az informatikai infrastruktúra egy Windows NT 4.0 tartományból áll. A tartomány egy elsődleges tartományvezérlőt (PDC) tartalmaz, amely a tartomány SAM adatbázisának mesterpéldányát tartalmazza. A tartomány egy, vagy több további másodlagos tartományvezérlőt tartalmazhat (BDC).

A tartomány egy Windows 2000 Active Directory tartománnyá migrálható. A Windows 2000 tartományon belül szervezeti egység tárolók (Organizational Unitok) hozhatók létre, melyeken keresztül a tartomány menedzselési feladatai jóval egyszerűbben megoldhatók.

2. Single Master Domain modell

Ez a tartományi modell több tartományból tevődik össze, melyek egyike mastertartománynak tekinthető. A mastertartomány tartalmazza a vállalat felhasználóinak felhasználói fiókjait (accountjait), valamint a globális csoportokat (Global Groups). A mastertartományhoz egy, vagy több erőforrásokat tartalmazó tartomány egyirányú megbízotti kapcsolattal (one-way trust relationship) kapcsolódik.

Tartományfrissítés esetén a modell Windows 2000 Active Directory fára (tree) alakítható át, ahol a master domain az Active Directory fa legfelső (root) tartományává válik.

Tartomány átszervezés esetén a Windows NT 4.0 tartományok az optimalizálási koncepciótól függően Windows 2000 szervezeti egységekké (OU) alakíthatók.

3. Multiple Master Domain modell

Ez a tartományi modell szintén több tartományból tevődik össze. Hasonló a Single Master Domain modellhez, azonban több mastertartományt tartalmaz. Az erőforrásokat tartalmazó tartományok valamennyi master tartomány felé egyirányú megbízotti kapcsolaton keresztül csatlakoznak.

Tartományfrissítés esetén a modell Windows 2000 Active Directory fára (tree) alakítható át. Ebben az esetben a tartományok egy újonnan létrehozott üres legfelső szintű (root) Windows 2000 tartomány alá kerülnek.

Tartomány átszervezés esetén a Single Master Domain modellhez hasonlóan a Windows NT 4.0 tartományok az optimalizálási koncepciótól függően Windows 2000 tartományokká, illetve szervezeti egységekké alakíthatók. A felhasználói fióko-

kat ebben az esetben célszerű a legfelső szintű tartományba áthelyezni.

4. Complete Trust Domain modell

Ebben a tartományi modellben több egyenrangú tartomány található, melyek kétirányú megbízotti kapcsolaton keresztül csatlakoznak.

Tartományfrissítés esetén a modell Windows 2000 Active Directory fára (tree) alakítható át. Ebben az esetben a tartományok egy újonnan létrehozott üres legfelső (root) Windows 2000 tartomány alá kerülnek. A kétirányú megbízotti kapcsolatok automatikus, tranzitív kapcsolatokként kerülnek kezelésre, csökkentve az erre irányuló adminisztratív feladatokat.

A követelményeknek megfelelően nagyobb fokú szétválasztási igény esetén (például egyéb szempontból különálló vállalkozások esetén) Windows 2000 erdő (forest) alakítható ki, ahol valamennyi Windows NT 4.0 tartomány egy különálló Windows 2000 legfelső szintű tartományt képez a saját tartományi fában.

A frissítés során a Windows NT-alapú tartományból az egyes objektumok az alábbiak szerint migrálódnak:

- A felhasználói fiókok (accountok) a users tároló (container) alá kerülnek.
- A számítógép fiókok a computers tároló alá kerülnek.
- A globális és lokális csoportok (global, local groups) a users tároló (container) alá kerülnek.
- A built-in csoportok a built-in tároló (container) alá kerülnek.

Az NTFS állományrendszerhez, nyomtatókhoz, lokális csoportokhoz tartozó hozzáférések (permission-ök) szintén migrálódnak.

Legfelső szintű tartomány (root domain) kialakítása

A legfelső szintű tartomány az Active Directory könyvtárszolgáltatások esetén a vállalat azonos tartományi névterületéhez (namespace) tartozó tartományi struktúrájának legfelső szintjén helyezkedik el (például microsoft.com).

Több tartomány esetén a fennmaradó tartományok hierarchikus módon a legfelső szintű tartomány altartományaiként (subdomain) kerülnek leképezésre.

A Windows NT 4.0 alapú infrastruktúrával már rendelkező vállalatok esetén – a Windows 2000 alapú infrastruktúrára történő áttéréskor – a legfelső szintű tartomány létrehozásával kapcsolatban két lehetőség kínálkozik.

- Egy már létező Windows NT 4.0 tartomány frissítése Windows 2000 legfelső szintű tartománnyá,
- új legfelső szintű Windows 2000 tartomány létrehozása.

A már létező Windows NT 4.0 tartományt Single, illetve Single Master tartományi topológia esetén legfelső szintű Windows 2000 tartománnyá lehet frissíteni.

Ha a tartományi topológia megváltoztatására vonatkozóan nem születik döntés, Multiple Master, illetve Complete Trust tartományi topológia esetén új, legfelső szintű Windows 2000 tartományként egy új tartomány létrehozása szükséges.

Előkészítési feladatok

A frissítési tevékenységek csak akkor indíthatók, ha a szükséges előkészítési procedúrák maradéktalanul elvégzésre kerültek. Ezek az előkészítő tevékenységek részben a migráció problémamentességét, részben pedig – esetleges problémák felmerülése esetén – a visszaállítási lehetőséget (rollback) biztosítják.

Minden frissítési tevékenység elindítása előtt a következő előkészítési tevékenységek elvégzésére van szükség:

- A rendelkezésre álló hardver vizsgálata erőforrás rendelkezésre állás (szabad merevlemez-kapacitás, memória-, processzorigény) és kompatibilitási szempontból.
- A frissítendő tartományvezérlőkön futó éles alkalmazások, kritikus szolgáltatások vizsgálata a frissítés szempontjából.
- Esetleges – nem várt – probléma esetére vonatkozó visszaállítási (rollback) forgatókönyv készítése.
- Teljes mentés végrehajtása.

A hardver és szoftver kompatibilitásának ellenőrzéséhez a Windows 2000 Compatibility Tool szintén használható. Az eszköz a kompatibilitási vizsgálat eredményeit szöveges állományban rögzíti.

Ezen túl kiszolgálók frissítése előtt célszerű az alábbi előkészítő feladatok elvégzése:

- Ideiglenesen távolítsuk el a kiszolgálókról a vírusvizsgáló, illetve egyéb állományrendszer szűrőket használó szoftvereket, harmadik gyártótól származó hálózati szolgáltatásokat, kliensprogramokat.
- Fizikailag válasszuk le az intelligens szünetmentes áramforrás soros csatlakozását.
- ISA (nem plug and play) eszközök esetén rezerváljuk valamennyi, a nem plug and play eszközök által használt megszakítást a számítógép BIOS-án keresztül.

Az előkészítési tevékenységeken túl fontosnak tartjuk kiemelni a tesztrendszerek, pilotmegoldások alkalmazását. Javasoljuk, hogy az „éles" környezet frissítése előtt lehetőleg teljesen azonos paraméterekkel felépített tesztrendszerben kerüljön végrehajtásra a migráció.

Bár a tesztrendszerek kiépítése többletkiadással jár, az üzemi környezet biztonságának, rendelkezésre állásának fenntartása ezt indokolttá teszi.

Visszaállítás tervezése

Minden frissítési tevékenység magában hordozza a problémák megjelenésének lehetőségét. Megfelelő visszaállítási (rollback) stratégia és rendszermentés nélkül az üzemi rendszerkörnyezet módosításához nem szabad hozzákezdeni.

A visszaállítási folyamat biztonságát, időigényének csök-

kentését a rendszer teljes mentésén túl „forró csere" kiszolgáló alkalmazása tovább fokozza.

A mentési procedúra részeként célszerű egy másodlagos tartományvezérlőre replikálni a directory adatbázist, majd leválasztani a hálózatról. Probléma esetén a kiszolgáló elsődleges tartományvezérlőként az „éles" rendszerbe visszahelyezve biztosítja a kiinduló rendszerállapot visszaállítását.

A frissítési folyamat

A koncepcionális és rendszertervezési, valamint előkészítési tevékenységek elvégzését követően sor kerülhet az operációs rendszerek frissítésére. A frissítési folyamat az alábbi fő lépésekből épül fel:

1. A Windows 2000 hálózat root domainjének létrehozása.
2. Elsődleges tartományvezérlők (Primary Domain Controllerek) frissítése.
3. Másodlagos tartományvezérlők (Backup Domain Controllerek) frissítése.
4. Tagkiszolgálók (member serverek) és kliens-számítógépek frissítése.
5. Áttérés vegyes módból (mixed mode) natív módba.

A migrációs folyamat az informatikai infrastruktúra méretétől (például kiszolgálók számától) függően hosszabb időt vehet igénybe.

A Windows 2000 operációs rendszer képes együttműködni a Windows NT 4.0 operációsrendszer környezettel. Ez az együttműködési lehetőség lehetővé teszi a fokozatos áttérést, időt engedve a vállalati informatika számára az optimális migráció lefolytatásához, valamint a vállalati felhasználók számára az új vállalati informatikai szolgáltatások megismeréséhez.

Miről frissíthetünk?

A Windows 2000 Professional verzióra történő frissítési tevékenységek az alábbi operációs rendszer verziókon hajthatók végre:

- Windows 9x
- Windows NT Workstation 3.51
- Windows NT Workstation 4.0

Windows 2000 Server, vagy Advanced Server verzióra a következő operációs rendszerek frissíthetők:

- Windows NT Server 3.51
- Windows NT Server 4.0

Tartományok frissítése

Abban az esetben, ha a vállalat több tartománnyal rendelkezik, a tartományok frissítését illetően célszerű frissítési sorrendet felállítani:

- Ha tartományi átszervezésre van szükség, az átszervezendő tartományok átalakításával kezdjük az áttérési tevékenységet. Ekkor első körben a felhasználói fiókokat tartalmazó tartományokat migráljuk.
- Felhasználói fiókotokat tartalmazó tartományok migrációjára esetén, a legkisebb fiókszámú, legalacsonyabb prioritású, legkönnyebben kezelhető tartományt frissítsük első lépésben.
- Erőforrástartományok esetén első lépésben azokat a tartományokat frissítsük elsőként, amelyek az új, Windows 2000-platform szolgáltatásokra támaszkodnak (például Exchange Platinum).

  Következő lépésben azokat a tartományokat frissítsük, amelyek nagyobb számú Windows NT-klienst tartalmaznak. Ebben az esetben a frissített géppark kihasználhatja a Windows 2000 infrastruktúra szolgáltatásait (például IntelliMirror).

Tartományvezérlők frissítése

A Windows NT 4.0 operációs rendszer verzióval ellentétben a Windows 2000 operációs rendszerben a tartományvezérlői szerepkör nem különül el elsődleges (PDC) és másodlagos tartományvezérlői (BDC) szerepekre.

Már létező Windows NT 4.0 tartomány esetén a frissítést az elsődleges tartományvezérlővel kell kezdeni.

A frissítés során a Windows 2000 operációs rendszer első indulásakor az Active Directory Installation Wizard (dcpromo.exe) automatikusan elindul, melynek segítségével az új tartomány jellemzői, valamint a felhasználók, csoportok és számítógép fiókok migrációja megoldható.

Az elsődleges tartományvezérlők frissítését követően sor kerülhet a másodlagos tartományvezérlők frissítésére.

A másodlagos tartományvezérlők frissítési procedúrája azonos az elsődleges tartományvezérlők frissítési folyamatával azzal a különbséggel, hogy az Active Directory Wizard futtatása esetén a kiszolgálót a korábbiakban már létrehozott tartományhoz kell hozzáadni.

Tagkiszolgálók frissítése

Tagkiszolgálók (member server) frissítésénél a kiszolgálói szerepkör megtartására, valamint tartományvezérlői szerepkörre történő áttérésre egyaránt lehetőség nyílik.

A frissítést követően a kiszolgáló továbbra is a frissítés előtt regisztrált tartomány vagy munkacsoport tagja marad. A kiszolgáló lokális felhasználói fiókjai és csoportjai nem migrálódnak az Active Directoryba.

A tagkiszolgálót a frissítést követően az Active Directory Installation Wizard segítségével tartományvezérlővé lehet előléptetni.

Abban az esetben, ha a tagkiszolgálón DHCP-szolgáltatás található, a frissítést követően azt az Active Directory szolgáltatások felé regisztrálni kell.

Áttérés vegyes módból natív módba

A Windows 2000 operációs rendszer tartományok kiszolgálói két különböző – vegyes, illetve natív – módban működhetnek.

Natív mód esetén valamennyi tartományvezérlőnek Win-

dows 2000 verzióval kell rendelkeznie. A tagkiszolgálókon és kliens munkaállomásokon továbbra is futtathatók a korábbi operációs rendszer verziók.

Vegyes mód alkalmazására az áttérési folyamat alatt a Windows 2000 és a Windows NT operációs rendszerek közötti kompatibilitás fenntartása miatt van szükség.

Vegyes mód esetén:

- A tartományvezérlőkön Windows NT és Windows 2000 verziók egyaránt működhetnek. Ebben az esetben a Windows NT operációs rendszert futtató kiszolgálók csak másodlagos tartományvezérlői szerepkört láthatnak el.
- Globális és lokális csoportok egyaránt értelmezettek, azonban a universal csoport nem alkalmazható.
- A csoportok egymásba ágyazására csak a Windows NT verziók esetén megismert módszerek alkalmazhatók, a Windows 2000 csoportkezelői funkcionalitás nem áll rendelkezésre.
- A Windows NT 4.0 system policy szolgáltatás a frissített Windows NT 4.0 számítógépeken továbbra is alkalmazható.
- Az Active Directory szervezeti egységek (OU-k) alkalmazhatók, azonban csak Windows 2000 adminisztrációs eszközök segítségével adminisztrálhatók
- Az IntelliMirror szolgáltatás működik, azonban csak Active Directory környezetben, Windows 2000 Professional kliensek esetén alkalmazható.
- A Kerberos authentikáció Windows 2000-alapú számítógépek esetén használható.
- A Group Policy szolgáltatás csak Windows 2000 Professional operációs rendszert futtató kliens munkaállomásokon alkalmazható.
- Két szervezeti egységben (OU) nem szerepelhet azonos user principal (felhasználói objektumok egyedi szöveges azonosítója) nevű felhasználó.

Abban az esetben, ha valamennyi tartományvezérlő frissítése megtörtént, a Windows 2000 tartomány átkapcsolható natív módba, ezáltal valamennyi Windows 2000 operációs rendszer szolgáltatás kihasználható.

A natív módra történő áttérés egy irányú, a vegyes módba történő visszatérésre nincs mód.

Munkaállomások frissítése

A kliens oldali számítógépek frissítési tevékenységei időben elválaszthatók a tartományvezérlők frissítési procedúráitól, mivel működésük az Active Directory-alapú szolgáltatásoktól függetlenek lehet.

A kliensek frissítése Windows 9x és Windows NT 3.51, illetve 4.0 verziók esetén közvetlenül lehetséges. Windows NT 3.1, valamint 3.5 verziók esetén a frissítést meg kell előzze egy fejlettebb Windows NT verzióra történő frissítés.

Azok a Windows 9x kliensek, amelyek hardverkompatibilitása nem megfelelő – a Directory Service Client szolgáltatás segítségével – operációs rendszer frissítése nélkül is használhatják az Active Directory directory services szolgáltatásait.

Az áttérés során alkalmazható további segédeszközök

Az áttérési tevékenység támogatására számos segédprogram, valamint „harmadik gyártó" által nyújtott hasznos támogatói megoldás létezik.

A segédeszközök alkalmazása hasznos, azonban minden esetben meg kell győződni az adott megoldás alkalmazhatóságáról, megbízhatóságáról.

Az alábbiakban harmadik gyártótól származó, illetve Microsoft által kifejlesztett, áttérést támogató segédeszközöket soroltunk fel:

- Entevo által fejlesztett megoldások (http://www.entevo.com/)
- FastLane által fejlesztett megoldások (http://www.fastlane.com/)
- NetPro által fejlesztett megoldások (http://www.netpro.com/)
- Mission Critical Software által fejlesztett megoldások (http://www.missioncritical.com/)
- ClonePrincipal
- MoveTree
- Netdom
- Robocopy
- PermCopy
- SIDWalker

Zárszóként.

A fenti fejezetekben megpróbáltuk áttekinteni az áttéréssel kapcsolatos főbb feladatköröket, folyamatokat, lehetőségeket...

...Körülbelül 22100 karakternél tartunk, így azt hiszem tovább már nem szabad fokozni az érdeklődést és leírhatom ☺:

A cikk terjedelme miatt természetesen technikai szempontból nem fejthettük ki mélyebben ezt az igen sok oldalon tárgyalható témakört, mondanivalónknak nem is ez volt az alapvető célja.

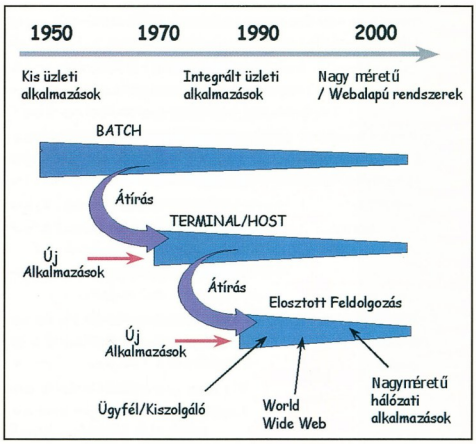
Ismét komolyra fordítva a szót remélem, hogy az áttekintő technikai információkon túl e pár oldal segítségével sikerült kifejeznem azt is, hogy az áttérés nem csupán egy technikai jellegű eseményt („upgrade-et") jelent, hanem egy olyan folyamatot, amely nagy figyelmet, gondos tervezést, előkészítést igényel, és végül a vállalati informatikai infrastruktúra magasabb minőségének eléréséhez vezet.

A cikket a szerző kérésének megfelelően változatlan formában, szerkesztés nélkül közöljük.

Elosztott alkalmazások fejlesztése DNA 2000-ben

dr. Charaf Hassan és Lenti Péter
hassan@aut.bme.hu
www.aut.bme.hu

Az egyik amerikai projektmegbeszélésen a megrendelő cég vezetője nekem szegezte a kérdést: – *„Hogyan tudjuk ezt a megoldani?“*
Tervezünk egy kártyát, és megírjuk hozzá a szoftvert – válaszoltam. Erre azt felelte: *„forget it, én csak a szabványos, skálázható, előre gyártott elemeken alapuló rendszerekben hiszek“*.



1. ábra **Alkalmazástípusok és technológiai trendek (Sterling Software, 1998)**

Az IT-ipar általában kétféle szempontból vizsgálja a megvalósítandó alkalmazásokat. Az egyik a rendszer kialakítása, „milyensége“, a másik pedig a fejlesztéshez használt módszer, a „hogyan“. Az első kérdésre napjainkban minden komolyabb fejlesztés esetében tévedhetetlenül az Internetalapú elosztott megközelítés (koncepció), a „hogyanra“ pedig manapság a komponensalapú módszer az elfogadott válasz, mivel ez a technika nagyon hatékony alkalmazásépítést tesz lehetővé.

A legózáshoz hasonló rendszerépítési iskola új gondolkodásmódot igényel a kódolás bűvkörében felnőtt szoftverfejlesztőktől. Arról nem is beszélve, hogy számos nehézséget (szabványos kommunikáció az előre gyártott elemek között, vegyes programozási nyelvek használata stb.) kellett megoldani, mielőtt jól működő komponensalapú rendszerek születhettek volna. Az *1. ábra* ötven évre visszatekintve a „szoftveriparosítás“ technológiai trendjeit szemlélteti.

A komponensalapú, elosztott alkalmazások fejlesztéséhez a Windows DNA (*Windows Distributed Internet Applications*) technológia egységes megoldást kínál.

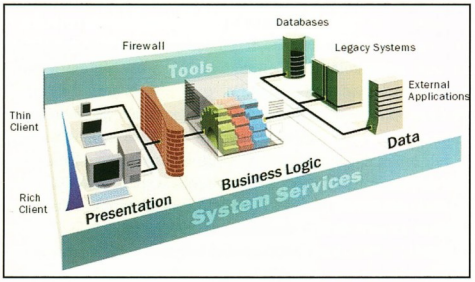
Mi is a Windows DNA?

Fejlesztési modell a Windows alatt futó alkalmazások elkészítéséhez. A DNA mindenre kiterjedő vázlatot ad ahhoz, hogy milyen eszközök és módszerek felhasználásával:

- fejleszthetünk robosztus, skálázható, elosztott, többrétegű alkalmazásokat Windows-platformon,
- hozhatunk létre megbízható webes alkalmazásokat,
- csatlakozhatunk szabványos interfészeken keresztül külső alkalmazásokhoz,
- szervezhetjük az alkalmazást funkció szerint több rétegbe.

Mik a Windows DNA előnyei?

• Egységes, nagy funkcióválasztékkal bíró alkalmazásszerver-platformot kínál az elosztott alkalmazások létrehozására. Ez a platform tartalmazza a középső réteg kialakításához szükséges közös szolgáltatásokat is, beleértve az aszinkron üzenetkezelést, a tranzakció-kezelést, a komponens-menedzsmentet, a just-in-time aktivizálást, valamint az adatbázis-kapcsolati eszközöket stb.



2. ábra **3 rétegű alkalmazás felépítése**

• Könnyebben és gyorsabban építhetjük meg alkalmazásunkat a Windows közös infrastrukturális szolgáltatásainak használatával.
• Többféle programozási nyelvvel és fejlesztési eszközparkkal alkalmazható.
• Messzemenőkig támogatja az együttműködést külső rendszerekkel.

A Windows DNA a három rétegű (3-tiered) elosztott alkalmazáshierarchiát javasolja, ami a *2. ábrán* is látható. A három réteg: megjelenítés, üzleti logika és adattárolás. A funkciók fizikai elosztásából adódóan a DNA koncepcióval épített rendszer ki tudja elégíteni a következő – a legtöbb nagy rendszer esetében elkerülhetetlenül szükséges – feltételeket.

Autonómia: a megjelenítési réteget teljesen el lehet választani a kritikus erőforrásoktól (pl.: adatbázis). Az adatokat csak megbízható (az üzleti logikát megvalósító) komponenseken keresztül lehet módosítani (ezek az összetevők a végrehajtók – lásd később). Köztük és a megjelenítési rész között a hatékonyabb működés céljából még további közvetítők is lehetnek, ezek a küldöttek.

Megbízhatóság: az MTS tranzakció támogatása (lásd később) lehetővé teszi, hogy az adatok mindig konzisztensek legyenek, és a kérések sose vesszenek el. Ez főleg többfelhasználós környezetben nagyon fontos.

Skálázhatóság: internetes környezetben nemritkán percenként több ezer kérést kell kiszolgálnia a rendszernek. Ahhoz, hogy erre képes legyen, feltétlenül szükséges, hogy a műveletek csak pillanatokig foglaljanak le egy-egy kritikus erőforrást. A méretezhetőségben kulcsszerepet játszik az MTS is, amely segít optimálisan megosztani az erőforrásokat.

Nagyobb rendelkezésre állás: a DNA a hardverhibákból eredő leállások kivédésére az NT RAID lehetőségét és a fürtözést ajánlja, az átmeneti hálózati hibák káros hatását pedig a Microsoft Message Queue Server segítségével tudjuk a minimálisra csökkentetni.

Együttműködés más platformon futó rendszerekkel: a DNA tanácsa szerint használjunk: ADO-t és/vagy OLE DB-t adathozzáféréshez; XML-t, hogy információkat cseréljünk más alkalmazásokkal; DCOM-ot, hogy elérjük más platformok – például Unix – alkalmazásait; MSMQ-t, hogy elérjük más platformok üzenetsorait és végül COM Transaction Integratort (COMTI), a tranzakció-végrehajtáshoz CICS (LU 6.2) rendszerekben.

Milyen részekből épül fel a Windows DNA?

A DNA nyílt szabványokra épülő komponensalapú alkalmazás-szolgáltatásokból és rendszerszolgáltatásokból áll, amelyek a COM technológiának köszönhetően képesek tökéletesen együttműködni. Íme néhány a DNA legfontosabb építőkövei közül:

• **megjelenítési szolgáltatások:** HTML, DHTML, XML, scriptek, win32 API;
• **alkalmazás-szolgáltatások:** Internet Information Server (IIS), Microsoft Message Queue Server (MSMQ), Microsoft Transaction Server (MTS), COM+, XML;
• **adatkezelési szolgáltatások:** Universal Data Access (UDO – magába foglalja többek között az ActiveX Data Objectset (ADO), és az OLE DB-t), XML;
• **rendszerszolgáltatások:** könyvtár, biztonság, menedzsment, kommunikáció;
• **eszközök:** tervezés, implementáció, telepítés.

A 2000. változat

A Windows DNA 2000, a DNA következő nemzedékének „igéi":

• *A fejlesztő a megoldandó feladatra koncentráljon, és ne az alapozással vesztegesse el az idejét!* A rendszer kész könyvtárakat kínál a gyakran ismétlődő funkciók elvégzésére (tranzakció-kezelés, SQL-lekérdezések, biztonságos adatcsere), így a programozó az egyedi üzleti–logikai részek megírására fordíthatja minden figyelmét.
• *Add a felhasználóknak, amit már megszoktak!* A DNA 2000 lelke a COM. Ezt a technológiát a legtöbb Windows programozó már jól ismeri, így DNA 2000-ben is gyorsan és hatékonyan tud dolgozni.
• *Csökkentsd a fejlesztés költségeit!* A korábbi DNA verzióból és a Windowsokból megismert technológiák egyesítésével és kibővítésével a DNA 2000 teljes szolgáltatásgyűjteményt kínál, ami sokkal olcsóbbá teszi a fejlesztést, a telepítést és a működtetést.

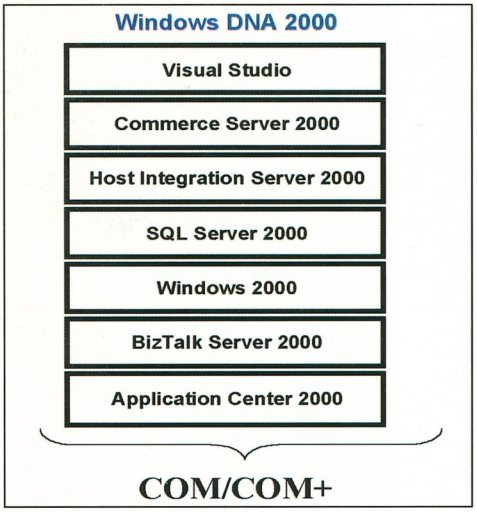
- *Használd fel a már meglévő rendszereket!* A DNA 2000 a legkülönfélébb rendszerekkel képes együttműködni, hiszen az alkalmazások szabványos interfészeket nyújtanak a külvilág számára.
- *Alkalmazkodj könnyen a gyorsan változó piaci igényekhez!* A DNA 2000 komponensalapú felépítésének köszönhetően könnyen és rugalmasan továbbfejleszthető.

A fenti kulcsszavakból is látható, hogy a Microsoft igyekezett az elektronikus üzleti rendszerek minden igényének megfelelni a Windows DNA 2000 kialakítása során.

A Windows DNA 2000 család

A DNA 2000 számos elemet nyújt, melyekre alkalmazásunkat építhetjük. Ezek az – egymással kiválóan együttműködő – egységek alkotják a Windows DNA 2000 családot, melynek képe a *3. ábrán* látható.

Az operációs rendszer (Windows 2000) a főpillér, erre építkezhetünk a további egységek szolgáltatásait a COM/COM+ segítségével igényeink szerint integrálva. Nézzük a különböző elemek szerepét!



3. ábra **Windows DNA 2000 család**

Microsoft Windows 2000

A Windows 2000 stabil és nagy teljesítményű. Ezen kívül az operációs rendszerbe integrálva tartalmazza az elosztott alkalmazások működéséhez szükséges funkciókat, ellentétben az előző Windows verziókkal, amelyek különválasztva kezelték ezeket. De miről is van szó?

- **COM+ szolgáltatások:** a COM összetevők továbbra is működnek a COM+ környezetben.
- **Webszerver:** Internet Information Server (IIS) 5.0 – gyorsabb adminisztráció és telepítés, címtárszolgáltatás, fürtözési szolgáltatás, erősebb biztonság, operációs rendszer szintű hálózati- és tranzakciós szolgáltatások jellemzik.
- **Active Server Pages (ASP):** ez olyan weboldal-generálási technológia, melynek segítségével a szerveroldali scriptekkel tudunk dinamikus, interaktív webes alkalmazásokat létrehozni.
- **Tranzakciók:** a Microsoft Transaction Server komponensalapú tranzakció-kezelő alrendszer, mely leveszi a programozó válláról annak összes terhét.
- **Üzenetkezelés:** a Microsoft Message Queue aszinkron üzenetsor kezelő szolgáltatás egyrészt segít csökkentetni a hálózati hibák hatását, másrészt lehetővé teszi az együttműködést más platformokon futó alkalmazásokkal (lásd később).
- **Adatelérés:** az ActiveX Data Objects technológia leegyszerűsíti az adatbázisok kezelését.
- **XML:** a Windows 2000 az első beépített XML-támogatással bíró Windows-változat.

  A támogatás azt jelenti, hogy kapunk egy – a W3C XML 1.0 szabványát követő – a XML Parser komponenst, amelyet scriptekbe építve kiválóan fel lehet használni a hordozható adatfile-ok kialakításához.

Microsoft Application Center 2000

Az Application Center 2000 új elem a Windows DNA 2000 családban; feladata a többszerveres rendszerek menedzselése, telepítése és diagnosztizálása.

Microsoft Host Integration Server 2000

A Host Integration Server 2000 lehetővé teszi a Windows-platform és más rendszerek (IBM mainframe, AS400, Unix) integrálását. Képes mindkét irányban közvetíteni a két „világ" között alkalmazás-, adat- és hálózati szinten is. Legfontosabb funkciói:

- Hálózati és biztonsági integrációs szolgáltatások:

  Az SNA Server technológiájára építve a HIS kezelni tudja az SNA-t és egyéb LAN protokollokat, valamint ezek kezeléséhez API-kat ad. Emellett beépített biztonsági szolgáltatásai is vannak, támogatja a jelszó-szinkronizációt és az egységes bejelentkezést az Active Directoryval együttműködve.

  A szolgáltatásokat terheléskiegyenlítő fürtökben is igénybe vehetjük.
- Adatintegrációs szolgáltatások:

  A Host Integration Server 2000 számos összetevőt tartalmaz, amelyek lehetővé teszik, hogy heterogén adatbázis-környezetben is elérhessük, kezelhessük és replikálhassuk adatainkat. Ezek közé tartoznak:

  •• Heterogén replikációs szolgáltatások:

  Kétirányú replikációt (merge, snapshot és incremental) hoz-

nak létre a Microsoft SQL Server, IBM DB2, és Oracle között.

•• ODBC és OLEDB szolgáltatók:
Elérhetővé tesznek több relációs és nem-relációs adatbázist, valamint file-rendszert (DB2, VSAM, AS400 file-rendszer, Oracle, és Sybase)

•• Host-initiated adatelérés:
Lehetőséget nyújt a DB2 fejlesztőknek, hogy úgy érjék el az SQL Servert, mintha DB2 adatforrás lenne.

- Alkalmazás-integrálási szolgáltatások:
A HIS az aszinkron (pl.: üzenetalapú) és a szinkron (például COM/DCOM) kommunikációt egyaránt támogatja. Emellett segít a fejlesztőknek, hogy a meglévő tranzakciókat és üzleti logikákat új elosztott alkalmazásokba fogják össze. Négy összetevőt tartalmaz:

•• COM Transaction Integrator (COMTI):
A COMTI által a CICS és IMS tranzakciós programok úgy érhetők el, mintha MTS vagy (kétfázisú commitot támogató) COM+ összetevők lennének. A COM+ komponensnek látszó programokat pedig már a „szokásos" COM összetevőkhöz hasonlóan bármilyen COM-ot ismerő fejlesztőeszközben felhasználhatjuk. A COMTI továbbá megengedi, hogy a CICS tranzakciók MTS tranzakciókat kezdeményezzenek.

•• XML Transaction Integrator (XMLTI):
A XMLTI XML interfészt ad a COMTI összetevők számára. Ez a lehetőség arra jó, hogy az XML-alapú dokumentumok és üzenetek (beleértve a BizTalk kompatibilis sémákat és üzeneteket) tranzakciókat kezdeményezzenek.

•• MSMQ to MQ Series Bridge:
Lehetővé teszi az üzenetcserét az IBM MQ Series és MSMQ formátumok között.

•• Host Integration Server 2000 SDK:
A Microsoft a HIS szolgáltatásainak igénybevételére SDK-t is kínál a fejlesztők számára. Ezzel az SDK-val a fejlesztők olyan újabb platformokat is integrálhatnak, amelyeket az alaptermék nem kezel.

Microsoft BizTalk Server 2000

A BizTalk Server 2000 olyan eszközöket és infrastruktúrát kínál, amelyek segítségével dokumentumokat tudunk cserélni a különböző platformok között attól függetlenül, hogy milyen alkalmazást használunk kezelésükre. Ezzel a családtaggal a vállalatok nemcsak a cégen belül használt különféle rendszerek között oldhatják meg a dokumentumok átvitelét, hanem az interneten keresztül üzleti partnereiknek is küldhetnek, illetve tőlük fogadhatnak megrendeléseket, számlákat és egyéb anyagokat.

A BizTalk adatcsere alapját a dokumentumokat leíró XML-alapú sémák adják. Ez a leírás vagy séma alapulhat a meglévő iparági szabványokon, például a vállalati beszerzésiken, valamint a hagyományos adatűrlapokon (ilyen például az EDI), vagy a termékkatalógusok, ajánlatok, reklámkampányok és más adatok újonnan kifejlesztett leírásán. Azoknak a vállalkozásoknak, amelyek használnak valamilyen űrlapot, általában már van üzleti folyamatokat támogató saját sémájuk.

A BizTalk fő újdonsága, hogy nemcsak a dokumentumok összeállítását segíti, hanem teljes keretrendszert nyújt a kezelésükhöz, továbbításukhoz és nyomon követésükhöz is. Ha betápláljuk a rendszerbe vállalatunk üzleti folyamatait, a hozzájuk tartozó jogosultságokat és a szükséges dokumentumcseréket, a többit a BizTalk már csaknem önműködően elvégzi.

Fontos, hogy ehhez olyan üzleti struktúrát kell kialakítanunk, melyben az alkalmazásszolgáltatások és az adatok lazán csatoltak – vagyis függetlenek és különállók. Ezáltal ha két rendszer között akarunk adatot cserélni, nem kell összehangolni a küldő és a fogadó infrastruktúráját, elég a dokumentum összeállítását és felvitelét megoldani.

A dokumentum összeállítása általában úgy történik, hogy valamelyik másik séma (például leltárűrlap) adatait képezzük le a kívántra (például szállítási űrlapra). Ez könnyű és pontosan nyomon követhető folyamat.

A lazán csatolt adatok módszerét használva a vállalkozások aránylag egyszerű struktúrájú üzleti alkalmazásokat és BizTalk rendszereket alakíthatnak ki, s ezeknek a tesztelése sem jelent kilátástalan feladatot. A közös adatok mellett közös logikát is használó vállalkozásintegrációs modelleknek jóval nagyobb a fejlesztési és a tesztelési igényük minden egyes kereskedelmi kapcsolat esetében.

A Microsoft Biztalk 2000-ben cégünk üzleti folyamatainak és a külső cégekkel fenntartott kapcsolatainak modelljét grafikus eszközzel tervezhetjük meg. Ugyancsak kényelmes alkalmazás segíti a dokumentumok és a dokumentum transzformációk összeállítását. A hiányzó lehetőségeket a BizTalk SDK-n keresztül könnyen kipótolhatjuk.

Microsoft Commerce Server 2000

A Commerce Server 2000 a Site Server 3.0 Commerce Edition utódja. Segítségével könnyen lehet ügyfélközpontú internetes, valamint extraneten működő kereskedelmi oldalakat létrehozni. Kifejlesztése során az a cél lebegett a tervezők szeme előtt, hogy a tulajdonos a lehető leghatékonyabb szolgáltatást tudja nyújtani az ügyfeleknek. Ennek eléréséért a CS egyrészt az új Online Analytical Processing (OLAP) komponens segítségével részletes statisztikát készít a felhasználói szokásokról, másrészt pedig minden eszközt megad ahhoz, hogy a weblap az egyes vásárlóknak testre szabott felülettel (és reklámokkal) szolgálhasson.

Microsoft SQL Server 2000

Az SQL Server legújabb verziója. A skálázhatósága, rendelkezésre állása, valamint menedzselhetősége is javult, továbbá támogatja az adattárházat/adatbányászatot és sok új e-kereskedelmi funkcióval is bővült. Jobban ki tudja használni a

Windows 2000 lehetőségeit, különösen a több processzort, a nagyobb memóriát, valamint a 64 bites hardverplatformot és a fürtözést.

Microsoft Visual Studio

Ez a népszerű fejlesztőeszköz-csomag, több programozási nyelvet és fejlesztő-környezetet tartalmaz. A csomagban képviselt nyelvek mindegyike képes illeszkedni a Windows DNA-platform elemeihez – például létrehozhatók és hívhatók velük a COM összetevők. A DNA 2000 alapú alkalmazások tervezéséhez és fejlesztéséhez a Visual Studio ideális választás.

Technikai/Technológiai háttér

A Windows DNA 2000 rövid bemutatása után térjünk rá a technikai és technológiai részletekre. Mint a Windows DNA 2000 családot bemutató ábrán is láthattuk, a COM/COM+ technológia a családtagok közös jellemzője. A COM+ a COM kiterjesztése.

Ha négy különböző fejlesztőtől kérdezzük a COM+ meghatározását, akkor négy különböző választ kapunk. Az egyértelműség kedvéért a COM+ a következő képlettel írható le:

COM + MTS(executants) + Szolgáltatások = COM+

Ezen a téren a fő újdonság abban rejlik, hogy a COM+ szolgáltatásai a Windows 2000 szerves részévé váltak.

COM

A Microsoft az NT 3.5-ös verziójával vezette be 32 bites, komponensalapú architektúráját, a Component Object Modelt. A COM a bináris file-ok formátumát leíró specifikáció, amely lehetővé teszi, hogy különálló programként működő, újrafelhasználható összetevőket, úgynevezett COM-szervereket hozzunk létre. Ezek különböző szolgáltatásokat tesznek elérhetővé más alkalmazások számára. A COM három legfontosabb alapelve a következő:

Az interfész és az implementáció elkülönítése: a komponensek szolgáltatásaikat interfészeken keresztül teszik elérhetővé a külvilág számára, a feladatuk megvalósításának módját viszont magukba zárják. Fejlesztéskor nem magát az összetevőt használjuk fel, hanem csak egy absztrakt szerkezetet – az interfészt, amely csak prototípusa a komponenseknek, implementációt nem tartalmaz. A komponens által végzett feladatokat az egy vagy több interfészt implementáló COM osztályok valósítják meg.

Függetlenség a programnyelvtől: a COM specifikációja két standard interfészt definiál, ezek csak arra szolgálnak, hogy egyáltalán hozzá tudjunk szólni valahogy a komponenshez. Ahhoz, hogy „jó is legyen valamire", további interfészeket kell létrehoznunk benne. Az **IUnknown** az egyik standard interfész; ez a COM összetevő életútját szabályozza, és ezen keresztül lehet a komponens által támogatott interfészek között is navigálni. A másik interfész az **IClassFactory**, mely az alkalmazás által kért objektum létrehozásáért és felszabadításáért felelős. Az interfészek létrehozására közös leírónyelv, a Microsoft Interface Definition Language (MIDL) szolgál. A leírásból fordítóprogram készíti el az interfész bináris képét – ez az objektum prototípusa.

Az objektum tényleges funkcióihoz az így elkészített interfészen keresztül, kétszeres indirekcióval, egy virtuális függvénytáblán keresztüli mutatóhivatkozással férhetünk hozzá. Vannak azonban olyan programozási nyelvek is (pl.: Visual Basic, script nyelvek), amelyek nem használnak pointereket. A megoldás, hogy implementáljuk az **IDispatch** interfészt, ekkor ez ellátja az objektum metódusait sorszámmal és névvel (ráadásul a listát akár futásidőben is lekérdezhetjük). Célszerű mindegyik interfészhez mindkét elérési módot implementálni, hiszen így mind Visual C++-ból, mind pedig Visual Basicből és scriptnyelvekből is elérhetők. Ezeket nevezzük dual interfészeknek (ezekhez az ATL nagy támogatást nyújt). Mivel a COM csak az interfész kialakítását szabja meg, az összetevők valódi funkcionalitását többféle programozási nyelvben (pl.: Visual C++, Visual Basic, Visual Java, Borland Delphi stb.) is megírhatjuk. Ugyanígy a COM azt sem korlátozza, hogy az összetevő funkcióit használó programot milyen nyelven valósítjuk meg.

Összetevők bináris szintű újrafelhasználása: régebben a programozók sok időt töltöttek olyan programmodulok implementálásával, amelyeket már korábban más programozók megvalósítottak. A legjobb esetben ezeknek a moduloknak a forráskódja elérhető volt számukra, de még ilyenkor is csak a kód beillesztésével és újrafordításával lehetett a kész programrészeket újra felhasználni; ráadásul a fordítóprogramok inkompatibilitása miatt ez a módszer rengeteg veszély forrása volt.

A COM-ban újrafordítás nélkül, bináris szinten lehet újrafelhasználni az összetevőket. Ez azt jelenti, hogy bármely programozási nyelven – fordítótól függetlenül – létrehozott bináris (lefordított) szoftverösszetevők szolgáltatásait bármely alkalmazás vagy további komponensek igénybe vehetik.

Az objektumoknak az azokat futtató szál elhelyezkedésétől függően két típusa van: a processzen belül (inprocess) és az azon kívül (out of process) futó. Az első esetben az objektum implementációja dinamikus könyvtárban (.DLL) található, ezt a felhasználó alkalmazás a saját memóriaterületén futtatja. A másik esetben a szerver külön processzben fut, és általában futtatható file (.EXE) formájában juthatunk hozzá.

A kliensalkalmazás távoli eljáráshívásokkal (RPC) kommunikál a szerverobjektummal. Ezeket a hívásokat a COM operációs rendszer szinten hajtja végre, a kliens számára teljesen transzparens módon. A processzen belüli szerver nagy hátránya, hogy ha az egyik oldalon hiba történik, mindkét program futása veszélybe kerül. Ez a megoldás nem kifejezetten biztonságos, cserében a metódushívások viszont gyorsak, mivel a hívó és a hívott memóriája közös. A processzen kívül futó összetevők hívása ezzel ellentétben meglehetősen lassúcska, ugyanis a két processz közötti összes hívásnak át kell haladnia az

operációs rendszeren. Ez utóbbi szervertípus viszont – mivel két külön processzről van szó – lehetővé teszi, hogy másik számítógépre helyezzük át az objektumot.

A Windows a registryben tárolt információk alapján határozza meg, hogy a kívánt COM szerverobjektum kódját tartalmazó dinamikus könyvtár vagy futtatható file hol található fizikailag. A regisztrációs adatbázis módosításával az összetevők fizikai helye a kliensek számára transzparens módon megváltoztatható.

A Windows DNA architektúra legfőbb erőssége skálázhatóságában rejlik. A három logikai réteg az alkalmazott technológiáknak köszönhetően (HTTP, DCOM, MSMQ, ADO) különböző számítógépre helyezhető.

Az üzleti logika eddig a kliens vagy a szerver számítógépeket terhelte (vastag, illetve vékony kliens), ezeknek az elsődleges feladata optimális esetben csak a megjelenítés, illetve az adattárolás lenne. Mivel az alkalmazáslogikát megvalósító összetevők ugyanúgy képesek működni attól függetlenül, hogy pontosan melyik – vagy hány – gépre tesszük őket, a rendszer középső rétege nagyon jól skálázható. Ha ugyanis a rendszer válaszideje nem megfelelő, a hálózat tetszőleges pontjára beállíthatunk új gépeket, és áttehetjük rájuk a komponensek egy részét, vagy további másolatokat telepíthetünk rájuk az összetevőkből.

Microsoft Transaction Server

A Windows DNA-ban az alkalmazáslogikát komponensek valósítják meg, melyeket több számítógépen is el lehet helyezni, így a terhelés megosztható, a rendszer skálázható. A komponensek elosztása a hálózaton két megoldandó kérdést vet fel. Az egyik az, hogy a telepítés és karbantartás erre alkalmas eszköz nélkül igen nehézkes és átláthatatlan. A másik, fontosabb gond a feldolgozás közben fellépő bonyodalmak kezelése.

A komponensek olyan összetett feladatokat látnak el, amelyek során esetleg adatbázisszerver, a file-rendszer vagy más komponensek szolgáltatásait is igénybe veszik. Ha valamelyik művelet elvégzése során hiba lép fel (hálózati kimaradás, hardverhiba stb.), a rendszer konzisztenciáját tranzakció-kezelés nélkül igen nehéz megőrizni. Ennek megoldására fejlesztették ki a Microsoft Transaction Servert, ez a Windows 2000-ben már az operációs rendszer része. Az MTS a logikailag összetartozónak értelmezett összetevőket egy csomagban kezeli, gondoskodik telepítésükről és a verziók karbantartásáról. Ezen kívül olyan környezetet is nyújt, amelyben a komponensek MTS objektumok felhasználásával – az adatbázis-kezelő szerverekhez hasonlóan – tranzakció-kezelést valósíthatnak meg.

Komponensek használata MTS nélkül: Ha kliensalkalmazásból használunk COM-szerver objektumot, a következő teendőink vannak a komponens életciklusát illetően:

- komponenspéldány létrehozása,
- a létrehozott példány inicializálása,
- a használata,
- az komponens törlése a memóriából használat után.

Ha az objektumot nem szabadítjuk fel explicit módon, akkor is törlődik a memóriából, miután kliensprogramunkból az utolsó hivatkozás is megszűnt. A COM objektumok memóriában tartása jelentős erőforrásokat foglalhat, ezért miután megtették kötelességüket, érdemes olyan gyorsan felszabadítani őket, amilyen gyorsan csak lehet. Ez a megközelítés azzal a hátránnyal jár, hogy ha újra igénybe szeretnénk venni az objektumot, akkor ismét létre kell hozni egy új példányt és inicializálni kell. Ez viszont jelentős időt vehet igénybe (gondoljunk csak a Word elindítására – ez szintén használható komponensként), úgyhogy sok esetben a programozó inkább úgy dönt, hogy a memóriában tartja a komponenst.

Összetevők az MTS alatt: Az MTS objektumkészlet (object pooling) alkalmazásával oldja meg a komponens példányok létrehozásának és törlésének nehézségeit. Ez az adatbázis-kapcsolatok használatához hasonlóan működik.

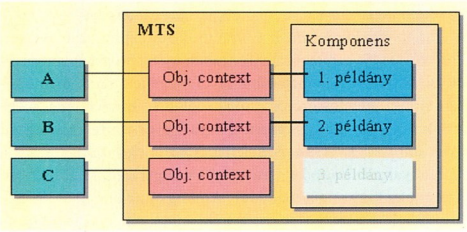
Az MTS lehetővé teszi, hogy más által létrehozott objektumpéldányt használjunk feltéve, hogy a létrehozó még nem szüntette meg explicit módon, de éppen nem is használja. Ha a létrehozó alkalmazás az érvényes interfész pointeren keresztül igénybe akarja venni az objektum valamelyik szolgáltatását – gondolván, hogy azt ő használja – az MTS „ellopja" egy másik alkalmazástól az egyik éppen inaktív példányt, és hozzárendeli a kérő klienshez. Az éppen inaktív példány tehát csak a kliens kérésekor aktiválódik (**just in time activation**), az MTS csak akkor hoz létre újabb példányt, ha nem talál megfelelő szabad egyedet az objektumtárban. Ezt a technikát nevezik állandó kontextusnak (**persistent context**), amelyre a következő eseménysorozat mutat példát:

Vegyünk a példa kedvéért három klienst (A, B és C), ezek a szerveren lévő komponensek példányaihoz kérnek hozzáférést. Első lépésként használjon **A** és **B** kliens egy-egy objektum példányt, és tegyük fel, hogy a **C** még nem hozott létre egyedet. (lásd *4/1. ábra*)

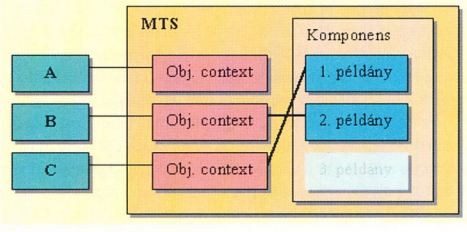
Ilyenkor az MTS lefordítja **A** és **B** kérését, és nem objektum példányokat, hanem virtuális kontextusokat hoz létre, valamint az objektum valós interfész pointerei helyett az ezekre mutató pointerekkel tér vissza a klienshez, azaz a kontextus mintegy megszemélyesíti az objektum interfészeit.

Következő lépésként tegyük fel, hogy **A** már nem használja a létrehozott objektumot, de még nem törölte explicit módon, azaz még fenntart rámutató érvényes interfész pointert. Amit valójában tart, az nem az komponenspéldány, hanem a kontextus objektum; a tényleges objektum példányt az MTS beteszi az objektumtárba, mint felhasználható példányt. Ha a **C** kliens új példányt kér ugyanebben az időben, akkor az MTS újabb kontextust hoz neki létre, de újabb példány helyett az **A**-tól elvettet rendeli hozzá (lásd *4/2. ábra*).

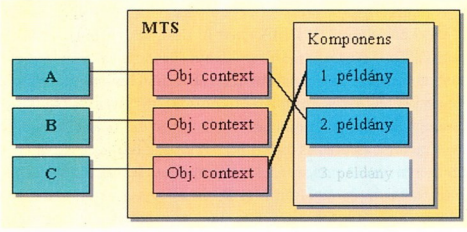
Tegyük fel, hogy **A** újra igénybe szeretné venni az összetevő szolgáltatásait. A létrehozott példányt szerencsétlenségére **C** használja, de ha **B** ugyanekkor végez a saját példányával,



4/1. ábra **Objektum kontextus**



4/2. ábra **Objektum kontextus**



4/3. ábra **Objektum kontextus**

akkor a Transaction Server az **A** kontextusához hozzárendeli **B** példányát olyan módon, hogy **A** észre sem veszi, hogy nem a saját példányát használja (lásd. *4/3. ábra*).

Az MTS csak akkor hozná létre az összetevő harmadik példányát, ha mindhárom kliens egyszerre válna aktívvá (jelen esetben akkor, ha **A** kérésekor nincs szabad példány az objektumtárban). A kérdés az, hogy az MTS mi alapján tudja megállapítani, hogy adott kliens használja-e még az objektumot. Ha a kliens explicit módon, azaz a rá hivatkozó változó *Nothing*-ra állításával (Visual Basic), vagy implicit módon, az ASP-oldal vagy processz feldolgozásának befejeződésével törli az objektumot, akkor az MTS értesül róla, hogy a példány bekerülhet az objektumtárba, és a kontextust megszüntetheti. De mikor rendelhető hozzá másik klienshez olyan példány, amelyre a létrehozó még rendelkezik referenciával?

Ha az összetevő a kliens kiszolgálását befejezte, akkor meghívja a kontextus objektum *SetComplete* vagy *SetAbort* metódusát. Az MTS ezáltal értesül arról, hogy az objektum befejezett egy taszkot, a belső állapotát már nem szükséges megtartani (vagy elküldte már a kliens felé, vagy a merevlemezen tárolódik a következő hívásig). Ezután a példány hozzárendelhető másik kliens processzhez.

Tranzakciók

Bár nem kizárt, hogy a komponensekre bontott rendszerek minden része egyetlen számítógépen helyezkedik el, általában inkább több gépen vannak elosztva, és távoli eljáráshívásokkal (COM Remote Procedure Call) kommunikálnak egymással. Ezért fontos, hogy egy komponens hibája ne legyen hatással a többi működésére, illetve ha hiba lép fel valamelyik elosztott művelet során, akkor a rendszer értelmes állapotban maradjon. Például, ha bankszoftvert írunk, ügyelni kell, hogy amennyiben átutalást hajtunk végre, és az egyik számláról már levontuk a pénzösszeget, azt biztosan adjuk hozzá a másikhoz is. Az tehát a kívánatos, hogy a felhasználó szemszögéből vagy a művelet minden része fusson le, és változtassa meg a rendszer állapotát, vagy hiba esetén a rendszer kerüljön vissza az eredeti állapotába, mintha nem történt volna semmi. Elosztott komponensek esetén nehéz megvalósítani az ilyenfajta hibakezelést, mert a folyamat számos hibalehetőséget rejt (pl.: a hálózati hozzáférés megszakad, a komponensek egyik részét futtató számítógép leáll stb.). A Windows DNA tranzakció-kezeléséről az MTS gondoskodik. Ez az összetevő valósítja meg a kliensek által kezdeményezett tranzakciókat. A tranzakciónak a kimenete vagy Commit (SetComplete) vagy RollBack (SetAbort) lehet.

ACID

A tranzakciónak – meghatározás szerint – meg kell felelnie az **ACID** tesztnek:

- **Atomic** – Atomi műveletként kell viselkednie, azaz csak akkor legyen hatása, ha a tranzakcióhoz tartozó összes művelet sikeres.
- **Consistent** – Akár sikeres, akár sikertelen, mindig olyan állapotban kell hagynia a környezetét, amely nem sérti annak integritását.
- **Isolated** – Ez a feltétel azt jelenti, hogy tranzakció eredményének meg kell egyeznie azzal az eredménnyel, amelyet akkor kapunk, ha a tranzakcióban szereplő műveleteket sorban egymás után hajtjuk végre (erre olyankor kell odafigyelni, amikor a tranzakció műveletei párhuzamosan hajtódnak végre).
- **Durable** – A tranzakció akkor állja ki e próbát, ha csak azután jelez sikert, miután minden egyes műveletének végeredménye megbízható tárolón rögzült. Ezáltal nem fordulhat elő, hogy rendszerhiba esetén a felhasználó azt hiszi, hogy a tranzakció sikeres volt, a végeredménye mégis elvész.

COM+

A COM+ a programozási modellként használt COM és a különálló MTS futtatási környezet egybeolvasztása megfűszerezve néhány további beépített szolgáltatással.

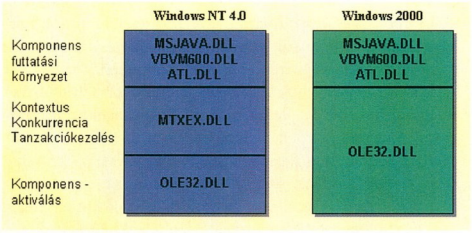
Ha NT 4 alatt futtatunk valamilyen alkalmazást, akkor az általa használt összetevőket a lefordításához használt fejlesztőeszköznek megfelelő dinamikus könyvtár szolgáltatásain keresztül éri el. A külön programként futó MTS az OLE32.DLL közbenjárásával veszi igénybe a COM objektumok szolgáltatásait. Windows 2000-platformon az MTS-t – egyéb szolgáltatásokkal egyetemben – a komponenseket menedzselő rendszerobjektumban valósították meg, így a COM+ funkciói az operációs rendszer szintjére kerültek.

A rendszer középső rétegének az a feladata, hogy fogadja a megjelenítési réteg kéréseit, és az adatelérési réteg szolgáltatásaira támaszkodva az üzleti logika szerint végrehajtsa őket, és az eredményt visszaadja a megjelenítési rétegnek. A Windows DNA középső rétege további két logikai részre oszlik: küldöttekre és végrehajtókra.

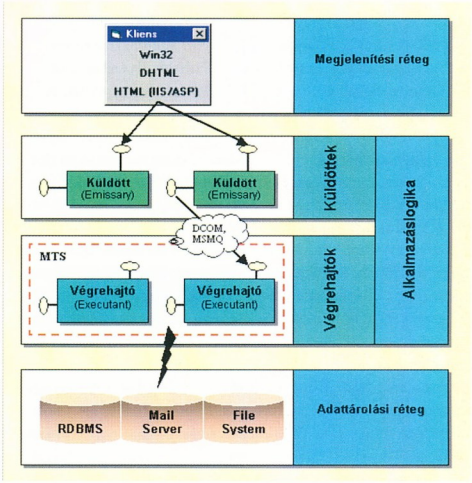
Végrehajtó: A DNA 2000 egyik fontos alapelve, hogy a kliens nem férhet hozzá közvetlenül a kritikus erőforrásokhoz (ilyen az adatbázis is). Ő csak a középső réteg üzleti logikájához fordulhat, amely ezután – ha úgy találja, hogy ez helyes és indokolt –, végrehajtja a nevében a szükséges műveleteket. Ez garantálja azt, hogy a „megbuherált" vagy hibás kliens ne ronthassa el az adatbázis tartalmát, és ne adhasson be inkonzisztens adatokat.

A kliensek kiszolgálásáról az üzleti logikát megvalósító és az adatkezelő réteggel kommunikáló végrehajtók felelősek. Joguk van írni és olvasni is az adatokat, a kliensek számára pedig csak olvasható pillanatképeket adhatnak az adatokról.

Küldött: A végrehajtó szó nélkül visszadob minden olyan kérést, amely nem tökéletes formátumú vagy hibás adatokat tartalmaz. Azért találták ki a küldötteket, hogy ne kelljen minden egyes kliensben újra megírni azokat a részeket, amelyek ellenőrzik, hogy a felhasználó (vagy külső rendszer) által megadott adatok megfelelnek-e a végrehajtó feltételeinek. Ezen kívül még azt is jelzik, hogy melyik részekkel van a gond. Emellett a küldöttek képesek további adatokkal is szolgálni a kliens



5. ábra **COM és MTS integráció**



6. ábra **Küldöttek és végrehajtók a Windows DNA 2000-ben**

számára, ugyanis van joguk olvasni (de csak olvasni) az adatkezelő réteg adatait.

A kliens tehát a küldöttel veszi fel a kapcsolatot, ez ellenőrzi a kérést, és ha megfelelő, továbbítja a végrehajtónak. A küldött és a végrehajtó közti kommunikációs csatorna megvalósításához többféle technika is használható (COM, MSMQ stb.).

Microsoft Message Queue Server

A fejlesztőket az elosztott rendszerek filozófiája arra késztette, hogy újra átgondolják az eddigiek során alkalmazott elveiket, és előrelépéseket tegyenek a következő területeken:

- A centralizált alkalmazások fejlesztése a mobil számítógépekre alapvető nehézség, ezekhez ugyanis a hálózati kapcsolat nem mindig áll rendelkezésre.
- Az internet és az elektronikus kereskedelem jelentősége rohamosan nő, ezért az alkalmazásokat fel kell rá készíteni, hogy a megbízható és biztonságos belső hálózat helyett a megbízhatatlan világhálón keresztül továbbítsák adataikat.
- Kell olyan eljárás, amely lehetővé teszi a különböző platformokon futó rendszerek kommunikációját.

Az előbb említett mindhárom gondot megoldja az az üzenetkezelő mechanizmus, amelyet a Windows-platformon a Microsoft Message Queue Server valósít meg.

Az MTS tranzakció-kezelése az elosztott rendszereket megbízhatóvá teszi ugyan, de az ennek során alkalmazott „mindent vagy semmit" elvnek van egy komoly hátránya is: mivel a számítógép-hálózatok sosem száz százalékos biztonsággal elérhe-

tők, ezért előfordulhat olyan eset, amikor az MTS alatt futó összetevő tranzakciója részeként távoli adatbázist szeretne módosítani, de a távoli szerver nem elérhető. Ilyenkor a tranzakció nem fejeződhet be, mert a kimenetele bizonytalan. A több órás vagy esetleg több napos várakozás elfogadhatatlan, mivel egyes lefoglalt erőforrások addig sem szabadulhatnak fel. Ez a megbízhatónak és gyorsnak tartott lokális hálózatokra (LAN) is érvényes, de még ennél is nagyobb gondot okoz az Interneten keresztül kommunikáló rendszerek esetében.

A kérdés üzenetkezelő rendszer bevezetésével oldható meg. Ez az e-mailhez hasonlóan működik: különböző platformok között is képes közvetíteni, és akkor is biztosítja az üzenetek célba érkezését, ha a címzett éppen nem elérhető.

Mivel Windows 2000-ről van szó, természetesen az üzenetkezelő rendszerek közül az MSMQ-t érdemes választani, mely magas szintű – a Windows 2000-ben már operációs rendszer – szolgáltatásokkal (kapcsolat más platformokkal, több protokoll támogatása, szinkron és aszinkron kommunikáció stb.) teszi az elosztott rendszert megbízhatóvá, skálázhatóvá és teljesítmény-orientálttá.

Kapcsolat nélküli kommunikáció

A folyamatos kommunikáció nem mindig megoldható két számítógép között. Vegyük például a hordozható számítógépet. A felhasználónak az lenne a legjobb, ha nem kellene minden művelet elvégzéséhez modemen keresztül becsatlakoznia a távoli szerverhez, hanem lokálisan tárolhatná, és egy csomagban elküldhetné a feldolgozásra váró információkat. Emellett azonban lehetővé kell tenni, hogy előbb-utóbb minden üzenet feldolgozásra kerüljön a távoli gépen, ezért az üzenetküldést tranzakciókba burkolva kell elvégezni (tértivevényes stílusban). A művelet első tranzakciója értelemszerűen a felhasználó értesítése arról, hogy a kérés feldolgozása megtörtént, azaz hogy a lokális üzenetsorba (message queue) került. A másik tranzakció az üzenet továbbítása és a távoli gépen történő feldolgozása. Az MSMQ technikája az e-mailhez hasonló: a felhasználó elküld egy levelet a saját levelezőszerverének (az előző példában a hordozható számítógép), amely továbbítja a címzett szerverének. Ha a címzett éppen nem csatlakozik a szerverhez, akkor a levél a következő csatlakozásig a mailboxban (message queue) tárolódik. A folyamat nyomon követhető az MSMQ-val együtt telepített MSMQ Intéző adminisztrációs segédprogram segítségével. Itt az adott számítógép összes üzenetsora, azok tulajdonságai, valamint az üzenetsorok által tartalmazott üzenetek is megtekinthetők.

Különböző platformokon futó programok kommunikációja

Az elosztott rendszerekben a felhasználói program, az összetevők és az adatbázis driverek COM, illetve ehhez hasonló technikával kommunikálnak egymással. Ha másik rendszert vagy összetevőt is be szeretnénk vonni az adatcserébe – olyant, amelyik nem támogatja ezeket a technikákat –, akkor közös interfészt kell bevezetni. Az üzenetalapú kommunikáció erre a célra is felhasználható. Az MSMQ csak Windows NT vagy Windows 95 alatt futtatható, azonban standard formátumú üzeneteivel platformfüggetlen üzenetkezelési rendszert valósít meg. Ahelyett, hogy közvetlenül az operációs rendszerekhez fordulna RPC hívásokkal, olyan formátumú üzeneteket alkalmaz, amelyeket minden rendszer értelmezni tud. A Level 8 Systems nevű cégtől lehet beszerezni olyan összetevőket, amelyek képesek üzeneteket cserélni más platformokon futó üzenetkezelő rendszerekkel (IBM MVS, MQ CICS, OS/2, AS/400, Sun Solaris, HP-Unix, AIX Unix).

Garantált egyszeri célba érkezés

Akárcsak a levelező-rendszerekben, az MSMQ esetén is fontos, hogy adott üzenet biztosan megérkezzen, és biztosan csak egyszer érkezzen meg a címzetthez. Ha az üzenet fogadása félbeszakad hálózati hiba vagy a fogadó számítógép meghibásodása miatt, akkor az MSMQ-nak értesülnie kell arról, hogy az üzenet fogadása sikertelen volt, és nem törölheti a sorból. Erre – mint azt az összetevők esetében láttuk – a tranzakciók alkalmazása a legjobb megoldás. A tranzakció keretein belül küldött üzenetek esetében nemcsak a sikeres célba érkezés garantált, hanem az is, hogy az üzenetek helyes sorrendben érkeznek meg.

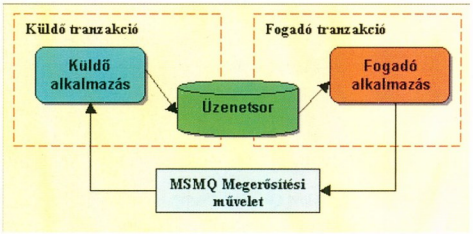
Ha az üzeneteket – jelzőbit beállításával – tranzakciókat támogató üzenetsoron keresztül továbbítjuk, akkor megvalósíthatjuk a biztos célba érkezésüket. Az MSMQ kétféle tranzakció-kezelést támogat. Van saját resource managere, amely lehetővé teszi, hogy az alkalmazások belső trtranzakciók (internal transactions) alatt küldjenek és fogadjanak üzeneteket. Ez a leghatékonyabb megoldás, mert gyorsabb és kevesebb erőforrást vesz igénybe, mint a külső resource managerek használata, viszont nagy hátránya, hogy csak az MSMQ üzenetek kezelésekor használható, külső tranzakciók kezelésekor nem. Ha az üzenet fogadása, illetve küldése sikeres, akkor az MSMQ belső Distributed Transaction Coordinatora (DTC) érvényesíti a tranzakciót. Ha a művelet során bármilyen hiba lép fel, akkor érvényteleníti azt, és lehetővé teszi, hogy az üzenetek visszakerüljenek az üzenetsorba, tehát a kezdeti állapot visszaálljon.

Az üzenetközvetítés módja

Az MSMQ kétféle közvetítési módot kínál: az expresszt és a visszaállíthatót (recoverable). A küldő alkalmazás választhat közülük. Az expressz üzenetek továbbítása gyorsabb és kevesebb erőforrást igényel, de mivel az MSMQ ezeket az üzeneteket a memóriában tárolja, ezért elveszhetnek. Például amikor valamelyik kliens a célalkalmazásnak az egyik MSMQ routing szerveren (lásd később) keresztül küld üzenetet, és a hálózat éppen nem elérhető a szerver és a cél között, akkor az elküldésre váró üzenetek a memóriában tárolódnak. Ha ilyenkor a szervert kikapcsoljuk, a memóriában tárolt üzenetek elvesznek,

és nem kerülnek elküldésre. Ezzel szemben a visszaállítható üzenetek a merevlemezen tárolódnak, és – az előbbi példával élve – a szerver visszakapcsolása után továbbításra kerülnek a kliens felé.

Az üzenetek tehát memóriában lévő (.MQ kiterjesztésű) file-okban tárolódnak. Az MSMQ minden visszaállítható üzenetet kiír a merevlemezre, az express üzeneteket pedig csak akkor, ha nincs elég szabad memória az üzenetek tárolására. Minden üzenet maximálisan 4 MB méretű lehet, és szöveget vagy bináris adatokat tartalmazhat.



7. ábra **Tranzakcionális üzenetközvetítés**

Loosely Coupled Events

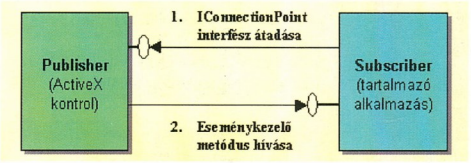
Az elosztott programozásban régóta megoldásra váró gond: hogyan kapcsolódhatunk olyan alkalmazáshoz, amelyben az adatok az idők során folyamatosan változnak, és milyen módon értesülhetünk ezekről a változásokról. A COM+ új eseményszolgáltatással, a **publish/subscribe** infrastruktúrával kínál lehetőséget ennek megoldására.

Az események generálása szempontjából ebben az esetben nem beszélhetünk a hagyományos értelemben vett kliensről és szerverről, ezért új elnevezéseket vezettek be: azt az alkalmazást, amely a változásról értesítést küld más programoknak *publishernek*; azt, amelyik megkapja ezt az értesítést és reagál rá, *subscribernek* nevezzük.

A hagyományos módszer ennek megvalósítására az elosztott programozásban a kliensoldali kapcsolódási pont létrehozása (eseménykezelés). Ez annyit jelent, hogy a subscriber a publisher számára elérhetővé tesz egy interfészt (IConnectionPoint), melyen keresztül a publisher a subscriber eseményt kezelő metódusát meghívhatja. Ezt a megközelítést használják az ActiveX kontrollok is az őket tartalmazó alkalmazások értesítésére (tightly coupled events).

Ez a mechanizmus csak abban az esetben működik, ha mindkét résztvevő egész idő alatt fut: attól kezdve, hogy a hívható interfészt a subscriber elérhetővé teszi egészen addig, amíg a publisher meghívja. A cél az, hogy a subscriber akkor is át tudja adni a hívási pontot, amikor a publisher éppen nem elérhető, és viszont: a publisher az értesítés küldésekor vagy aktiválni tudja az éppen nem élő címzettet, vagy el tudja helyezni a hívást üzenetsorban. A másik gondot az jelenti, hogy a subscribernek mindig pontosan ismernie kell azt az értesítési módot, amelyet a publisher használ, tehát ezt kell valamilyen egységes, minden subscriber számára érthető formára hozni. A harmadik nehézség forrása az, hogy a címzettek nem tudják megválogatni, melyik üzeneteket kapják meg, így minden értesítést fogadnak. Ezekre a kérdésekre a saját mechanizmus kifejlesztése nem lehet megoldás, mert különböző programozók által megvalósított rendszerekben biztosan különböző módszereket találnánk. A megoldás tehát az, hogy az operációs rendszer szolgáltatását kell erre igénybe venni.

A COM+ eseménykezelése már a Windows 2000 operációs rendszer szintű szolgáltatása, amely lehetővé teszi a publisher és a subscriber aszinkron módon történő összekapcsolását. A publisher bármely program lehet, amely COM hívásokat generál (COM-kliens), a subscriber pedig a hívott COM-szervert megvalósító alkalmazás. A klasszikus eseménykezeléshez képest az a különbség, hogy a rendszer eseményszolgáltatása beszkelődik a két résztvevő közé. Ez tartja nyilván, hogy mely subscriberek mely értesítéseket kívánják megkapni, valamint ez továbbítja az üzeneteket is. A COM+-ban a két fél közti kapcsolat „esemény osztályon" (event class) keresztül jelenik



8. ábra **Publisher és subscriber szinkron eseménykezeléssel**

meg. Ez olyan COM+ interfész, amelynek metódusait a publisher meghívja az esemény generálásakor, és amelyet a subscribernek implementálnia kell az üzenet fogadásához.

A COM+ vagy adminisztratív eszközön keresztül, vagy akár magától a publishertől értesül arról, melyek azok az interfészek és metódusok, amelyeket az adott esemény osztálynak tartalmaznia kell. Ezt az interfészek bináris leírását tartalmazó type library rendelkezésre bocsátásával teszi meg. A subscriber a megfelelő adatok elküldésével mondhatja meg, hogy melyik eseményosztály mely interfészétől és annak melyik metódusától kíván értesítést kapni. Az előjegyzésnek két fajtája van: az állandó előjegyzések megmaradnak az operációs rendszer újraindítása után is, a tranziens előjegyzések azonban nem. Amikor a publisher eseményt generál, a COM-ban már megszokott módon (CreateObject és CoCreateInstance hívásokkal) hozza létre az objektumot, azonban az objektum nem a megszokott módon aktiválódik. A COM+ a híváskor kikeresi a katalógusból az összes subscribert, amelyek erre az eseményre elője-

gyeztek, és mindegyiket minden lehetséges módon (az összetevő aktiválásával, üzenetkezeléssel stb.) értesíti a hívásról.

A rendszer jelenlegi implementációjának két jelentős hiányossága van. Először is, több számítógép esetén nem lehet elosztott esemény-katalógust kialakítani, így az összes publishert közös számítógépen kell regisztrálni, és a subscriberek erről a közös pontról kapják meg az értesítést.

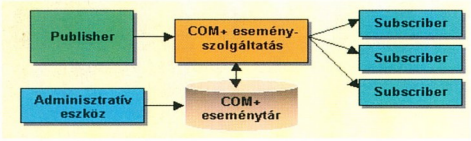
Ez azt jelenti, hogy az értesítés nem az optimális útvonalon halad, hanem mindig a kijelölt központi számítógépen keresztül, ami nagy mennyiségű hálózati forgalmat eredményez.

A másik, jelentősebb nehézség az, hogy centrális elrendezés esetén a rendszernek van egy hibaérzékeny pontja: ha a központi gép hiba folytán kiesik, akkor az eseménykezelés teljesen megbénul.

Queued Components

Az elérhetőség szempontjából az elosztott szoftverek esetén nem szerencsés, ha a működésükhöz alapfeltétel, hogy a rendszer minden összetevője folyamatosan rendelkezésre álljon. Ezt a gondot olyan aszinkron metódushívási mechanizmus oldhatná meg, melyben a hívásokat valamilyen közbülső réteg regisztrálja, és amikor a másik fél ismét elérhető, továbbítja annak. Ez a fajta architektúra a szerveroldali erőforrások gazdaságosabb kihasználását és a skálázhatóság javítását egyaránt lehetővé teszi.

Az aszinkron modell kialakítására a COM+ az MSMQ szolgáltatásaira épülő üzenetkezelési technikát alkalmaz. Az ilyen



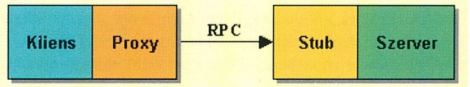
9. ábra **COM+ esemény-szolgáltatás**

módon működő komponensek neve Queued Components. A kliens a már megszokott módon hozza létre a szerver objektum egy példányát, a szerver pedig olyan interfészeket tesz elérhetővé, mint a szinkron COM összetevők.

A COM a hívások továbbítására szinkron RPC hívásokat alkalmaz. Ezzel szemben a COM+, a két fél közé helyezi az MSMQ-t, azaz a hívásokat aszinkron üzenetekként továbbítja.

A COM+ aszinkron szolgáltatásának kihasználása a programozók részéről tehát nem jelent semmiféle külön munkát, az eddig megszokott módon kell implementálni az összetevőket, és az alkalmazott architektúra a rendszer részeinek rendelkezésre állásától függetlenül, aszinkron módon futtatja azokat. Mégis van néhány megkötés az implementációra a modell aszinkron voltából következően:

- az interfészek metódusai csak bemeneti paramétereket használhatnak,

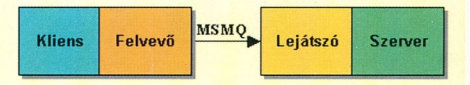


10. ábra **Szinkron COM hívás**

- paraméterátadás csak érték szerint történhet, referencia szerint nem
- alkalmazás-specifikus HRESULT visszatérési értékek nem használhatók.

Activation-time Load Balancing

A COM+ összetevők a terhelés kiegyenlítése céljából úgy konfigurálhatók, hogy a klienseknek az objektumok létrehozá-



11. ábra **Queued Components**

sára szolgáló CoCreateInstance hívásai routeren keresztül jussanak el adott Windows 2000-et futtató COM+ clusterhez. Ez a router figyeli a clusterben elhelyezkedő szerverek terheltségét, és a kért objektumot azon a számítógépen hozza létre, amelynek válaszideje a legkisebb.

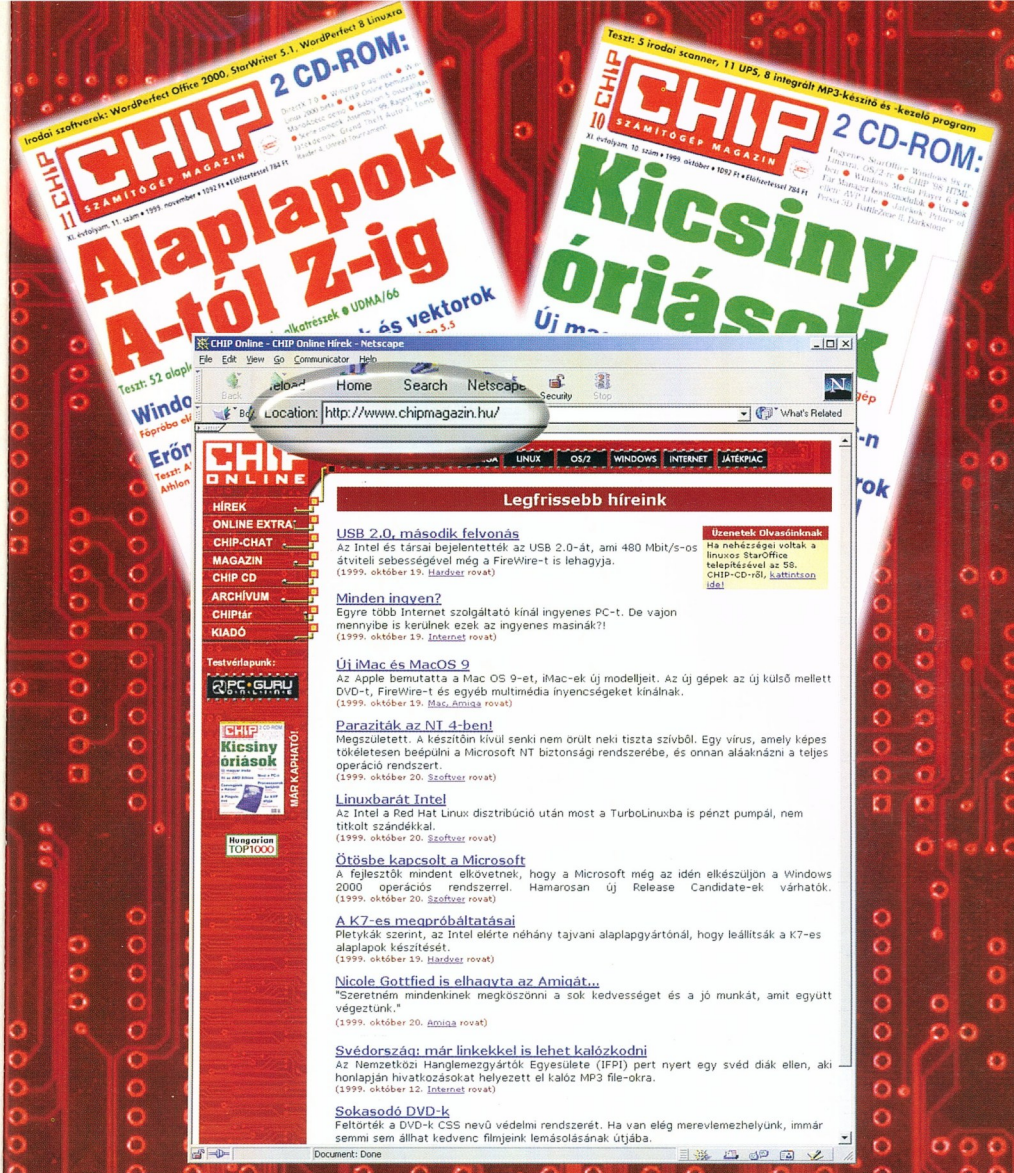
Ennek beállítása csak a kliensgép regisztrációs adatbázisának módosítását jelenti; azt a routert kell megadni futtató számítógépként, amely a válaszidő mérését végzi. Ha egyszer ez alapján az objektum az egyik szerveren létrejött, akkor a további hívások ugyanannak a szervernek továbbítódnak, amíg a példány meg nem szűnik.

Zárszó

E cikknek az volt a célja, hogy összefoglalja a Windows DNA 2000 lényegét, és bemutassa a legfontosabb részeit. Terjedelmi okok következményeként nem tudtunk minden részletre kitérni, így forráskód darabkákat sem mutattunk be. Reméljük, azért az előző néhány oldallal hozzájárultunk a Windows DNA 2000 jobb megértéséhez.

Mutatók

DNA:	www.microsoft.com/dna
UDO:	www.microsoft.com/data
MTS:	www.microsoft.com/transaction
Host Integration Server:	www.microsoft.com/sna
Biztalk:	www.biztalk.org
	www.microsoft.com/biztalk


Irodai szoftverek: WordPerfect Office 2000, StarWriter 5.1, WordPerfect 8 Linuxra
CHIP
SZÁMÍTÓGÉP MAGAZIN
2 CD-ROM:
Alaplapok
A-tól Z-ig
Teszt: 5 irodai scanner, 11 UPS, 8 integrált MP3-készítő és -kezelő program
2 CD-ROM:
Kicsiny
óriások
CHIP Online - CHIP Online Hírek - Netscape
File Edit View Go Communicator Help
Home Search Netscape Security Stop
Location: http://www.chipmagazin.hu/
What's Related
CHIP ONLINE
LINUX OS/2 WINDOWS INTERNET JÁTÉKPIAC
HÍREK
ONLINE EXTRA
CHIP-CHAT
MAGAZIN
CHIP CD
ARCHÍVUM
CHIPtár
KIADÓ
Testvérlapunk:
PC-GURU
MÁR KAPHATÓ!
Hungarian TOP1000
Legfrissebb híreink
USB 2.0, második felvonás
Az Intel és társai bejelentették az USB 2.0-át, ami 480 Mbit/s-os átviteli sebességével még a FireWire-t is lehagyja.
(1999. október 19. Hardver rovat)
Üzenetek Olvasóinknak
Ha nehézségei voltak a linuxos StarOffice telepítésével az 58. CHIP-CD-ről, kattintson ide!
Minden ingyen?
Egyre több Internet szolgáltató kínál ingyenes PC-t. De vajon mennyibe is kerülnek ezek az ingyenes masinák?!
(1999. október 19. Internet rovat)
Új iMac és MacOS 9
Az Apple bemutatta a Mac OS 9-et, iMac-ek új modelljeit. Az új gépek az új külső mellett DVD-t, FireWire-t és egyéb multimédia ínyencségeket kínálnak.
(1999. október 19. Mac, Amiga rovat)
Paraziták az NT 4-ben!
Megszületett. A készítőin kívül senki nem örült neki tiszta szívből. Egy vírus, amely képes tökéletesen beépülni a Microsoft NT biztonsági rendszerébe, és onnan aláaknázni a teljes operáció rendszert.
(1999. október 20. Szoftver rovat)
Linuxbarát Intel
Az Intel a Red Hat Linux disztribúció után most a TurboLinuxba is pénzt pumpál, nem titkolt szándékkal.
(1999. október 20. Szoftver rovat)
Ötösbe kapcsolt a Microsoft
A fejlesztők mindent elkövetnek, hogy a Microsoft még az idén elkészüljön a Windows 2000 operációs rendszerrel. Hamarosan új Release Candidate-ek várhatók.
(1999. október 20. Szoftver rovat)
A K7-es megpróbáltatásai
Pletykák szerint, az Intel elérte néhány tajvani alaplapgyártónál, hogy leállítsák a K7-es alaplapok készítését.
(1999. október 19. Hardver rovat)
Nicole Gottfied is elhagyta az Amigát...
"Szeretném mindenkinek megköszönni a sok kedvességet és a jó munkát, amit együtt végeztünk."
(1999. október 20. Amiga rovat)
Svédország: már linkekkel is lehet kalózkodni
Az Nemzetközi Hanglemezgyártók Egyesülete (IFPI) pert nyert egy svéd diák ellen, aki honlapján hivatkozásokat helyezett el kalóz MP3 file-okra.
(1999. október 12. Internet rovat)
Sokasodó DVD-k
Feltörték a DVD-k CSS nevű védelmi rendszerét. Ha van elég merevlemezhelyünk, immár semmi sem állhat kedvenc filmjeink lemásolásának útjába.
Document: Done
NEM HELYETTE,
MELLETTE!
www.chipmagazin.hu

A VOGEL PUBLISHING KFT. LAPJAI ÁTFOGJÁK A VILÁGOT

Media made by Vogel

Vogel Publishing Kft., 1139 Budapest, Hajdú u. 42–44., tel./fax: 350-8731